21世纪高职高专规划教材

计算机应用系列

Windows Server 2003网络管理

姜玉波 张海林 孙鹏 郑自国 卢俏立 孙晓晗 编著

清华大学出版社

21世纪高职高专规划教材

计算机应用系列

Windows Server 2003网络管理

姜玉波　张海林　孙　鹏
郑自国　卢俏立　孙晓晗　编著



清华大学出版社
北　京

内 容 简 介

本书浓缩了作者多年计算机网络教学改革与应用的实践经验。按照教学及学生学习知识的规律，作者对本书的章节顺序进行了合理编排，做到先基础后应用，通过形象的语言和丰富的图片、表格，全面地介绍了 Windows Server 2003 的网络功能。全书的主要内容包括：网络技术基础，DNS 服务器、DHCP 服务器、Web 服务器、FTP 服务器、电子邮件服务器、新闻服务器的原理、安装、配置和管理，流媒体服务，即时通信服务，索引服务。部分章节配有疑难解答及上机实战。

本书适合作为高等院校计算机网络应用课程，也可作为本科、高职高专、成人教育、计算机培训的教材，以及供计算机网络自学者、爱好者阅读使用。

图书在版编目(CIP)数据

Windows Server 2003 网络管理/姜玉波等编著. —北京：清华大学出版社，2010.10
(21 世纪高职高专规划教材.计算机应用系列)
ISBN 978-7-302-23564-4

Ⅰ.①W… Ⅱ.①姜… Ⅲ.①服务器—操作系统(软件)，Windows Server 2003
Ⅳ.①TP316.86

中国版本图书馆 CIP 数据核字(2010)第 158231 号

责任编辑：张龙卿
责任校对：刘 静
责任印制：

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185×260　　**印　　张**：16.25　　**字　　数**：393 千字
版　　次：2010 年 10 月第 1 版　　**印　　次**：2010 年 10 月第1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：031399-01



前　　言

Windows Server 2003 是服务器操作系统，它包含了用户希望从 Windows 服务器操作系统中所获得的全部功能特性。本书以 Windows Server 2003 标准版为例，详细地介绍了 Windows Server 2003 的网络功能。

本书共分为 10 章。第 1 章介绍了网络的基本功能，主要包括计算机网络的体系结构，网络服务器的体系结构和技术指标、7 种常见的网络设备工作原理、网络安全技术、TCP/IP 的测试等；第 2 章介绍了 DNS 服务器的配置与管理，主要包括 DNS 服务器的工作原理、配置和管理，以及创建和设置 DNS 区域、建立和管理 DNS 资源记录；第 3 章介绍了 DHCP 服务器的配置与管理，主要包括 DHCP 服务器的安装、创建和设置 DHCP 作用域、DHCP 客户端的设置；第 4 章介绍了 Web 服务器的配置和管理，主要包括 Web 服务器的安装、Web 网站的管理和配置、网站安全及实现；第 5 章介绍了 FTP 服务器的配置和管理，主要包括建立和配置 FTP 站点、打造 SSL 安装加密的 Serv-U 服务器；第 6 章介绍了电子邮件服务器的配置和管理，主要包括 MDaemon 邮件服务器的安装、配置和管理，以及通过 WorldClient 实现 Web 邮件服务；第 7 章介绍了新闻服务，主要包括新闻服务概述、安装 DNews 服务器端的配置与安装、客户端访问新闻服务器的方法；第 8 章介绍了流媒体服务，主要包括流媒体概述、Windows Media 服务的安装和基本配置、如何使用 Windows Media 提供点播服务；第 9 章介绍了即时通信服务，主要包括 FreeICQ 服务器端和客户端的安装、设置、基本应用；第 10 章介绍了索引服务，主要包括索引引擎概述、微软索引服务的工作原理和特点、管理索引服务、建立和维护索引、索引查询等。

本书是编者根据多年的教学经验及实践经验编写的，对章节的编排也是根据认识规律，由简到繁，由易到难，对 Windows Server 2003 主要的服务器的介绍都是先介绍原理，再介绍如何安装、配置，最后是如何进行管理。这样读者很容易抓住这一条规律，很自然地掌握每一种服务器的功能。本书内容循序渐进，结构清晰，层次分明，通俗易懂，通过大量的图片、表格来说明服务器的安装、配置的步骤。另外，为了使读者更好地掌握各章节的内容，每章末配有疑难解答和适量精选的习题，部分章还配有上机实战。通过本书的学习和练习，读者既能迅速掌握网络的基础知识，又能很快地学会各种服务器的配置、安装与管理技术，提高了解决实际问题的能力。

本书由姜玉波、张海林、孙鹏、郑自国、卢俏立和孙晓晗编著。第 1 章、第 4 章和第 5 章由张海林编写，第 2 章和第 3 章由孙鹏编写，第 6 章和第 7 章由郑自国编写，第 8 章和第 9 章由卢俏立编写，第 10 章由孙晓晗编写，全书由姜玉波统稿。另外，冯宁、郑砚、李龙、杨小



勇等也参加了部分内容的编写和校对工作，在此一并表示感谢！

本书在编写过程中参考了大量的有关 Windows Server 2003 的书籍及资料，在此对参考文献的作者表示衷心的感谢、

由于作者水平有限，书中难免存在错误或不当之处，恳请广大读者批评指正，以便再版时改进。

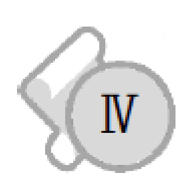
编　者

2010 年 6 月



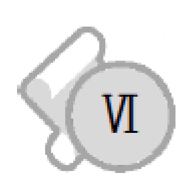
目　　录

















第1章　网络技术基础

本章要点

- 了解网络服务器的技术指标
- 了解 OSI 参考模型及各层的功能
- 掌握 TCP/IP 参考模型及各层的功能
- 了解常见网络设备的功能
- 掌握 IP 地址的分类及各自用途
- 了解网络安全措施
- 掌握常用网络测试命令

随着网络应用的日益普及,我们不能只满足于简单的页面浏览、在线视频等应用,还要对书籍、报纸、杂志、媒体上的一些网络相关的名词和术语加以了解,这样才能跟得上时代的发展。本章就从网络服务器、网络体系结构、网络设备、网络安全、网络测试等方面对日常生活中接触到的相关术语加以详细描述。

1.1　了解网络服务器

网络服务器是指在网络环境下运行相应的应用软件,为网上用户提供共享信息资源和各种服务的一种高性能计算机,英文名称叫做 Server。常见的网络服务器为客户机/服务器(Client/Server)模式,如图 1-1 所示。其中,客户机请求服务,服务器处理和提供服务。服务器可以提供数据库服务、文件服务、检索服务和其他各种各样的应用服务。具体分类如下。

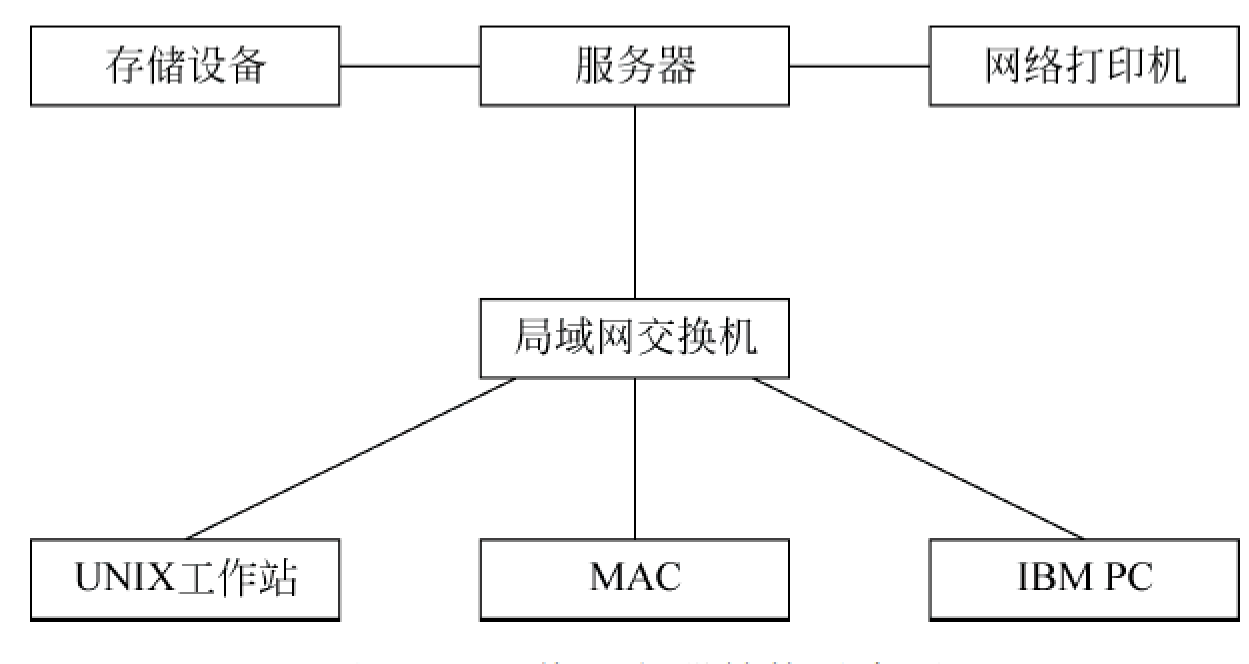


图 1-1　网络服务器结构示意图



1. 文件服务

通过网络，客户能将文件服务器中的共享文件下载到自己的计算机中，客户也能将自己的文件上传到文件服务器中。在 Internet 中，文件传输协议(FTP)就是专门提供文件服务的。文件服务是网络中最基本的网络服务，例如建立共享文档库、共享程序库、共享图像库、共享视频库、共享音频库等。

2. 数据库服务

数据库服务是网络中最重要的组成部分，通过网络，客户能查询数据库服务器中的数据，数据库服务器处理客户的 SQL 请求，将查询的结果传送给客户。由于数据库系统中存储着大量重要的企业管理数据，因此，数据库服务器显得特别重要。

3. Web 服务

Web 服务广泛应用于 Internet/Intranet 网络中，采用浏览器/服务器(Brower/Server)网络计算模式，浏览器/服务器是客户机/服务器网络计算机模式的继承和发展。用户通过浏览器网络，可浏览 Web 服务器的文字、图像、视频、音频等信息。

4. 电子邮件服务

电子邮件服务是世界上使用最为广泛的 Internet 服务。据统计，目前每天约有 8000 万人发送电子邮件，内容可以是商业备忘和科学研究讨论等。使用电子邮件服务器，客户能有效地交流信息和通信。

5. 应用服务

根据用户的需求，可设置各种不同的应用服务器，例如视频服务器、音频服务器、CAD 服务器等。服务器发展到今天，适应各种不同功能、不同环境的服务器不断地出现，分类标准也多种多样。按应用层次划分，可把服务器分为入门级服务器、工作组级服务器、部门级服务器和企业级服务器四类。按服务器的用途划分，可把服务器分为通用型服务器和专用型服务器两类。按服务器的机箱结构来划分，可把服务器分为台式服务器、机架式服务器、机柜式服务器和刀片式服务器四类。

1.1.1 服务器硬件体系结构

服务器是一种高性能的计算机，它的构成与我们平常所用的计算机有很多相似之处，诸如有 CPU、内存、硬盘及各种总线等，只不过它能够提供网络、Web 应用、数据库、文件、打印等各种共享服务。

由于服务器是针对网络应用特别定制的，因而服务器又与普通计算机在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面存在很大的区别。最大的区别就是在多用户多任务环境下的运行可靠性上。用计算机当作服务器的用户都经历过突然的停机、意外的网络中断、存储数据不时丢失等事件，这都是因为计算机的设计没有保证过多用户多任务环

境下的可靠性，所以一旦发生严重故障，其所带来的经济损失将是难以预料的。但一台服务器所面对的是整个网络的用户，需要每天 24 小时不间断地工作，所以它必须具有极高的稳定性。另外，为了实现高速稳定的运转，服务器通过采用对称多处理器安装、插入大量的高速内存来保证其正常运行。

服务器的主板可以同时安装几个甚至几十个 CPU，采用的内存无论在容量，还是性能、技术等方面都与普通计算机有根本的不同。另外，服务器为了保证足够的安全性，还采用了大量普通计算机没有的技术，如冗余技术、系统备份、在线诊断技术、故障预报警技术、内存纠错技术、热插拔技术和远程诊断技术等，使绝大多数故障能够在不停机的情况下得到及时的修复。服务器与普通计算机的比较如表 1-1 所示。

表 1-1　服务器与普通计算机的比较

指　　标	服　务　器	普通计算机
处理器性能	支持多处理，性能高	一般不支持多处理，性能低
I/O（输入/输出）性能	强大	相对弱小
可管理性	高	相对低
可靠性	非常高	相对低
扩展性	非常强	相对弱

1.1.2　服务器的技术指标

服务器常见的技术指标如下。

1. 服务器 CPU

服务器 CPU 是在服务器上使用的 CPU。服务器是网络中的重要设备，要接受成千上万用户的访问，因此对服务器具有大数据量的快速吞吐、超强的稳定性、长时间运行等严格要求。所以说 CPU 是衡量服务器性能的首要指标。

2. 服务器内存

服务器内存与普通计算机内存在外观和结构上没有明显的区别，主要是在内存中引入了一些特有的技术，如 ECC、ChipKill、Register、热插拔技术等，具有极高的稳定性和纠错性能。

3. 服务器硬盘

对用户来说，存储在服务器上的数据是最宝贵的，因此硬盘的可靠性是非常重要的。为了使硬盘能适应大数据量、超长工作时间的工作环境，服务器一般采用高速、稳定、安全的 SCSI 硬盘。

4. 服务器操作系统

服务器操作系统也叫网络操作系统，与运行在工作站上的操作系统有差别。一般情况下，网络操作系统是以使网络相关特性最佳为目的，如共享数据文件、软件应用以及共享硬盘、打印机、调制解调器、扫描仪和传真机等。一般的操作系统，其目的是系统的易用性。



目前主要存在以下三类网络操作系统。

- Windows 类。微软公司的 Windows 系统不仅在个人操作系统中占有绝对优势，它在网络操作系统中也有很大的市场。这类操作系统在局域网中是最常见的，但由于它对服务器的硬件要求较高，且稳定性能不是很高，因此微软的网络操作系统一般只用在中低档服务器中，高端服务器通常采用 UNIX、Linux 等非 Windows 操作系统。
- UNIX 类。目前常用的 UNIX 系统版本主要有 UNIX SUR4.0、HP-UX 11.0 等。UNIX 系统支持网络文件系统服务，提供数据等应用，功能强大。这种网络操作系统稳定和安全性能非常好，但由于它多数是以命令方式进行操作的，对初级用户来说不易掌握。因此，小型局域网基本不使用 UNIX 作为网络操作系统，UNIX 一般用于大型的网站中。
- Linux 类。这是一种新型的网络操作系统，它最大的特点就是源代码开放，可以免费得到许多应用程序。目前也有中文版本的 Linux，如 RedHat、红旗 Linux 等。Linux 在国内得到了用户的充分肯定，主要体现在它的安全性和稳定性方面，它与 UNIX 有许多类似之处。但目前这类操作系统主要应用于中、高档服务器中。

5. 应急管理端口

应急管理端口英文缩写为 EMP，全称是 Emergency Management Port，是服务器主板上所带的一个用于远程管理服务器的接口。远程控制机可以通过调制解调器与服务器相连，控制软件安装在控制机上。远程控制机通过 EMP Console 控制界面可以对服务器进行打开或关闭服务器的电源、重新设置服务器和监测服务器等工作。

6. RAID

RAID 是英文 Redundant Array of Independent Disks 的缩写，即独立磁盘冗余阵列，也称为磁盘阵列。

7. SMP

SMP 全称是 Symmetrical Multi-Processing，即对称多处理技术，是指在一台计算机上汇集了一组处理器，各处理器之间共享内存和总线结构。这是一种应用十分广泛的并行技术。在这种架构中，一台计算机不再由单个 CPU 组成，而是由多个处理器运行操作系统，并共享内存和服务器上的其他资源。

8. 容错技术

所谓容错，是指在硬件或软件出现故障时，仍能完成处理和运算，不降低系统性能，即用冗余的资源使计算机具有容忍故障的能力。这可以通过硬件和软件方法来实现。

1.2　计算机网络体系结构

计算机网络由多个互联的节点组成，节点之间要不断地交换数据和控制信息。要做到有条不紊地交换数据，每个节点就必须遵守一整套合理而严谨的结构化管理体系。计算机



网络就是按照高度结构化设计方法采用功能分层原理来实现的。

1.2.1 网络体系结构的基本概念

网络体系结构是用分层研究方法定义的网络各层的功能、各层协议和接口的集合，最早是由 IBM 公司在 1974 年提出的，名为 SNA。遵循该网络标准的设备可以很方便地实现互联。

而后，很多公司相继建立自己的网络体系结构，大大加快了计算机网络技术的发展。但随之而来的问题是，由于标准不同，各公司不同的网络体系结构之间的互联产生阻碍。

国际标准化组织(ISO)于 1977 年成立专门机构，提出了一个使各种计算机在世界范围内能够互联成网络的标准框架——开放系统互联基本模型(Open System Interconnection Reference Model，OSI/RM)。

1.2.2 ISO/OSI 参考模型及各层的功能

开放系统互联基本模型是由国际标准化组织(ISO)制定的标准化开放式计算机网络层次结构模型，又称 ISO/OSI 参考模型。OSI 包括了体系结构、服务定义和协议规范三级抽象。OSI 的体系结构定义了一个七层模型，用以进行进程间的通信，并作为一个框架来协调各层标准的制定；OSI 的服务定义描述了各层所提供的服务，以及层与层之间的抽象接口和交互用的服务原语；OSI 各层的协议规范精确地定义了应当发送何种控制信息及何种过程来解释该控制信息。

OSI 参考模型自下而上的模型结构如图 1-2 所示。从图中可见，整个开放系统环境由作为信源和信宿的端开放系统及若干中继开放系统通过物理媒体连接构成。这里的端开放系统和中继开放系统，都是国际标准 OSI7498 中使用的术语。通俗地说，它们相当于资源子网中的主机和通信子网中的节点机(IMP)。只有在主机中才可能需要包含所有七层的功能，而在通信子网中的节点机一般只需要最低三层甚至只要最低两层的功能就可以了。

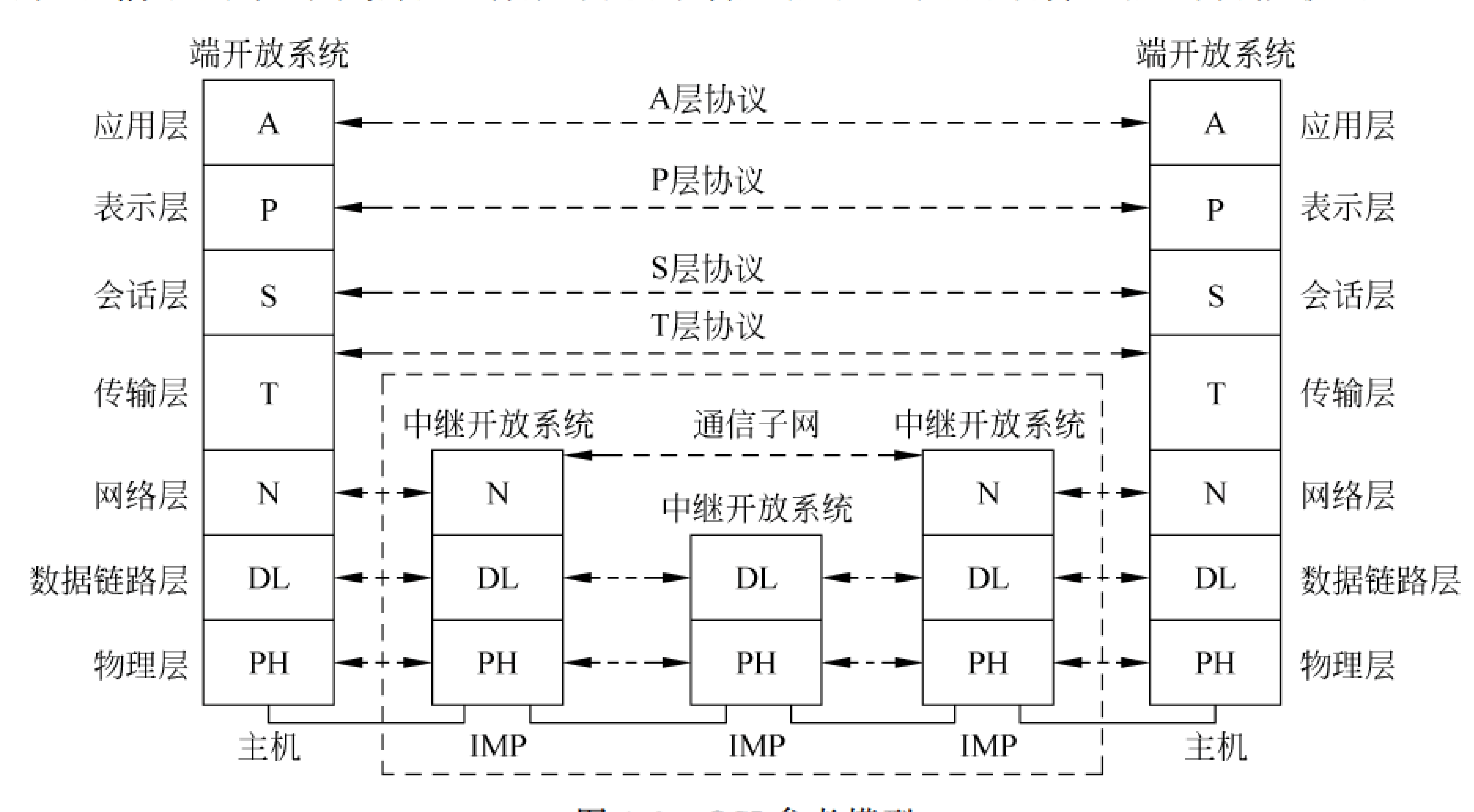


图 1-2 OSI 参考模型



OSI 参考模型各层的功能如下。

1. 物理层

物理层定义了为建立、维护和拆除物理链路所需的机械、电气、功能和规程的特性，其作用是使原始的数据比特流能在物理媒体上传输。具体涉及接插件的规格，0、1 信号的电平表示，收发双方的协调等内容。

2. 数据链路层

比特流被组织成数据链路协议数据单元（通常称为帧），并以其为单位进行传输，帧中包含地址、控制、数据及校验码等信息。数据链路层的主要作用是通过校验、确认和反馈重发等手段，将不可靠的物理链路改造成对网络层来说无差错的数据链路。数据链路层还要协调收发双方的数据传输速率，即进行流量控制，以防止接收方因来不及处理发送方来的高速数据而导致缓冲器溢出及线路阻塞。

3. 网络层

数据以网络协议数据单元（分组）为单位进行传输。网络层关心的是通信子网的运行控制，主要解决如何使数据分组跨越通信子网从源地址传送到目的地址的问题，这就需要在通信子网中进行路由选择。另外，为避免通信子网中出现过多的分组而造成网络阻塞，需要对流入的分组数量进行控制。当分组要跨越多个通信子网才能到达目的地址时，还要解决网际互联的问题。

4. 传输层

这是第一个端对端，也即主机对主机的层次。传输层提供的端到端的透明数据运输服务，使高层用户不必关心通信子网的存在，由此用统一的运输原语书写的高层软件便可运行于任何通信子网上。传输层还要处理端到端的差错控制和流量控制问题。

5. 会话层

这是进程对进程的层次，其主要功能是组织和同步不同的主机上各种进程间的通信（也称为对话）。会话层负责在两个会话层实体之间进行对话连接的建立和拆除。在半双工情况下，会话层提供一种数据权标来控制某一方何时有权发送数据。会话层还提供在数据流中插入同步点的机制，使得数据传输因网络故障而中断后，可以不必从头开始而仅重传最近一个同步点以后的数据。

6. 表示层

表示层为上层用户提供共同的数据或信息的语法表示变换。为了让采用不同编码方法的计算机在通信中能相互理解数据的内容，可以采用抽象的标准方法来定义数据结构，并采用标准的编码表示形式。表示层管理这些抽象的数据结构，并将计算机内部的表示形式转换成网络通信中采用的标准表示形式。数据压缩和加密也是表示层可提供的表示变换功能。

7. 应用层

该层是开放系统互联环境的最高层。不同的应用层为特定类型的网络应用提供访问



OSI 环境的手段。网络环境下不同主机间的文件传送访问和管理(FTAM)、传送标准电子邮件的处理系统(MHS)、使不同类型的终端和主机通过网络交互访问的虚拟终端(VT)协议等都属于应用层的范畴。

1.2.3　TCP/IP 参考模型及各层的功能

TCP/IP 参考模型是因特网(Internet)的基础。和 OSI 的 7 层协议比较,TCP/IP 参考模型中没有会话层和表示层。通常说的 TCP/IP 是一组协议的总称,TCP/IP 实际上是一个协议族(或协议包),包括 100 多个相互关联的协议。其中 IP(Internet Protocol,网际协议)是网络层最主要的协议;TCP(Transmission Control Protocol,传输控制协议)和 UDP(User Datagram Protocol,用户数据报协议)是传输层中最主要的协议。一般认为 IP、TCP、UDP 是最根本的三种协议,是其他协议的基础。

Internet 上使用的一个关键的底层协议是网际协议,也称 IP 协议。利用一个共同遵守的通信协议,使 Internet 成为一个允许连接不同类型的计算机和不同操作系统的网络。要使两台计算机彼此之间进行通信,必须使两台计算机使用同一种"语言"。通信协议就是两台计算机交换信息所使用的共同语言,它规定了通信双方在通信中共同遵守的约定。

TCP 协议是一种端对端的协议。当一台计算机需要与另一台远程计算机连接时,TCP 协议会让它们建立一个连接、发送和接收数据以及终止连接。

TCP 协议利用重发技术和拥塞控制机制,向应用程序提供可靠的通信连接,使它能够自动适应网上的各种变化。Internet 是一个庞大的国际性网络,网络上的拥挤和空闲时间总是交替不定的,加上传送的距离也远近不同,所以传输数据所用时间也会变化不定。TCP 协议具有自动调整的功能,能很好地适应 Internet 上各种各样的变化,确保传输数据的正确。

综上所述,虽然 IP 和 TCP 这两个协议的功能不尽相同,也可以分开单独使用,但它们是作为一个协议体系来设计的,并且在功能上也是互补的。只有两者的结合,才能保证 Internet 在复杂的环境下正常运行。凡是要连接到 Internet 的计算机,都必须同时安装和使用这两个协议,实际应用中这两个协议统称为 TCP/IP 协议。

TCP/IP 也是使用协议栈来工作,栈是所有用来在两台机器间完成一个传输的所有协议的几个集合。数据通过栈,从一台机器到另一台机器,在这个过程中,一个复杂的查错系统会在起始机器和目的机器中执行。栈分成五个层,每一层都能从相邻的层中接收或发送数据,每一层都与许多协议相联系。

TCP/IP 参考模型的各层功能如下。

- 网络接口层。为 TCP/IP 参考模型的底层,是 TCP/IP 的实现基础,其中可包含 MILNET、IEEE 802.3 的 CSMA/CD、IEEE 802.4 的 Token Bus 以及 IEEE 802.5 的 Token Ring。
- 网络互联层,相当于 OSI 参考模型中的网络层。IP 为网际协议(Internet Protocol)、ICMP 为国际控制报文协议(Internet Control Message Protocol)、ARP 为地址转换协议(Address Resolution Protocol)、RARP 为反向地址转换协议(Reverse ARP)。
- 传输层,负责在应用进程之间的端—端通信。TCP 为传输控制协议,UDP 为用户数据报协议(User Datagram Protocol)。



- 应用层,相当于 OSI 参考模型中的 5～7 层。

1.2.4　OSI 和 TCP/IP 体系结构比较

OSI 和 TCP/IP 的相同点是二者均采用层次结构,而且都是按功能分层。二者的区别如下。

- OSI 分七层,而 TCP/IP 分四层。严格讲,TCP/IP 网间网协议只包括下三层,应用程序不属于 TCP/IP 的一部分。
- OSI 层次间存在严格的调用关系,两个(N)层实体的通信必须通过下一层(N－1)层实体,不能越级,而 TCP/IP 可以越过紧邻的下一层直接使用更低层次所提供的服务(这种层次关系常被称为“等级”关系)。因而减少了一些不必要的开销,提高了协议的效率。
- OSI 只考虑用一种标准的公用数据网将各种不同的系统互联在一起,后来认识到互联网协议的重要性,才在网络层划出一个子层来完成互联作用。而 TCP/IP 一开始就考虑到多种异构网的互联问题,并将互联网协议 IP 作为 TCP/IP 的重要组成部分。
- OSI 开始偏重于面向连接的服务,后来才开始制定无连接的服务标准,而 TCP/IP 一开始就有面向连接和无连接服务,无连接服务的数据报对于互联网中的数据传送以及分组语音通信都是十分方便的。
- OSI 与 TCP/IP 对可靠性的强调也不相同。对 OSI 的面向连接服务,数据链路层、网络层和传输层都要检测与处理错误,尤其在数据链路层采用校验、确认和超时重传等措施提供可靠性,而且网络和运输层也有类似技术。而 TCP/IP 则不然,TCP/IP 认为可靠性是端到端的问题,应由传输层来解决,因此它允许单个的链路或机器丢失数据或数据出错,网络本身不进行错误恢复,丢失或出错数据的恢复在源主机和目的主机之间进行,由传输层完成。由于可靠性由主机完成,增加了主机的负担。但是,当应用程序对可靠性要求不高时,甚至连主机也不必进行可靠性处理,在这种情况下,TCP/IP 网的效率最高。
- 在两个体系结构中智能的位置也不相同。OSI 网络层提供面向连接的服务,将寻径、流控、顺序控制、内部确认、可靠性带有智能性的问题,都纳入网络服务,留给末端主机的事就不多了。相反,TCP/IP 则要求主机参与几乎所有网络服务,所以对入网的主机要求很高。
- OSI 开始未考虑网络管理问题,到后来才考虑这个问题,而 TCP/IP 有较好的网络管理。

1.3　常见网络设备介绍

1.3.1　中继器

中继器是网络物理层上面的连接设备,工作于 OSI 参考模型的物理层,是局域网上所有节点的中心,它的作用是放大信号、补偿信号衰减、支持远距离的通信。适用于完全相同





的两类网络的互联，主要功能是通过对数据信号的重新发送或者转发，来扩大网络传输的距离。

中继器是扩展网络的最廉价的方法。当扩展网络的目的是要突破距离和节点的限制时，并且连接的网络分支都不会产生太多的数据流量，成本又不能太高时，就可以考虑选择中继器。

由于传输线路噪声的影响，承载信息的数字信号或模拟信号只能传输有限的距离，中继器的功能是对接收信号进行再生和发送，从而增加信号传输的距离。它是最简单的网络互联设备，连接同一个网络的两个或多个网段。如以太网常常利用中继器扩展总线的电缆长度，标准细缆以太网的每段长度最大 185m，最多可有 5 段，因此增加中继器后，最大网络电缆长度则可提高到 925m。一般来说，中继器两端的网络部分是网段，而不是子网。

使用中继器有如下限制条件：

- 要保证中继器能够正确工作，首先要保证每一个分支中的数据包和逻辑链路协议是相同的。例如，在 802.3 以太局域网和 802.5 令牌环局域网之间，中继器是无法使它们通信的。
- 中继器只将任何电缆段上的数据发送到另一段电缆上，并不管该数据中是否有错误或是否适合于在该网段上传输。
- 采用中继器连接网络分支的数目，要受具体的网络体系结构限制。
- 中继器没有隔离和过滤功能，它不能阻挡含有异常的数据包从一个分支传到另一个分支。这意味着，一个分支出现故障可能影响到其他的每一个网络分支。

1.3.2　集线器

集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。它工作于 OSI 参考模型的第一层，即物理层。集线器与网卡、网线等传输介质一样，属于局域网中的基础设备，采用 CSMA/CD(一种检测协议)访问方式。

Hub 是一个多端口的转发器，当以 Hub 为中心设备时，网络中某条线路产生了故障，并不影响其他线路的工作。所以 Hub 在局域网中得到了广泛的应用。大多数的时候它用在星型与树型网络拓扑结构中。

Hub 按照不同的说法有很多种类。按照对输入信号的处理方式，可以分为无源 Hub、有源 Hub、智能 Hub。具体介绍如下。

1. 无源 Hub

它不对信号做任何的处理，对介质的传输距离没有扩展，并且对信号有一定的影响。连接在这种 Hub 上的每台计算机，都能收到来自同一 Hub 上所有其他计算机发出的信号。

2. 有源 Hub

有源 Hub 与无源 Hub 的区别就在于它能对信号放大或再生，这样它就延长了两台主机间的有效传输距离。



3. 智能 Hub

除具备有源 Hub 所有的功能外，还有网络管理及路由功能。在智能 Hub 网络中，不是每台机器都能收到信号，只有与信号目的地址相同地址端口的计算机才能收到。有些智能 Hub 可自行选择最佳路径，这就对网络有很好的管理。

在环型网络中，只存在一个物理信号传输通道，都是通过一条传输介质来传输的，这样就存在各节点争抢信道的矛盾，传输效率较低。引入集线器这一网络设备后，每一个站点是用它自己专用的传输介质连接到集线器的，各节点间不再只有一个传输通道，各节点发回来的信号通过集线器集中，集线器再把信号整形、放大后发送到所有节点上，这样至少在上行通道上不再出现碰撞现象。

当然，集线器也有缺点。基于集线器的网络仍然是一个共享介质的局域网，这里的“共享”其实就是集线器内部总线，所以当上行通道与下行通道同时发送数据时仍然会存在信号碰撞现象。当集线器将从其内部端口检测到碰撞时，产生碰撞强化信号向集线器所连接的目标端口进行传送。这时所有数据都将不能发送成功，形成网络“大塞车”。这是因为在集线器中，虽然各节点与集线器的连接已有各自独立的通道，但是在集线器内部却只有一个共同的通道，上、下行数据都必须通过这个共享通道发送和接收数据，这样有可能像单车道一样，当上、下行通道同时有数据发送时，就可能出现塞车现象。

正因为集线器的这一不足之处，所以它不能单独应用于较大网络中，通常是与交换机等设备一起分担小部分的网络通信负荷。因为网络越来越复杂，出现网络碰撞现象的机会就越大。也正因如此，集线器的数据传输效率是比较低的，因为它在同一时刻只能有一个方向的数据传输，也就是所谓的“单工”方式。如果网络中要选用集线器作为单一的集线设备，则网络规模最好在 10 台以内，而且集线器带宽应为 10/100Mbps 以上。

集线器除了共享带宽这一不足之处外，还有一个方面在选择集线器时必须要考虑到，那就是它的广播方式。

由于集线器属于纯硬件网络底层设备，基本上不具有类似于交换机的智能记忆能力和学习能力。它也不具备交换机所具有的 MAC 地址表，所以它发送数据时都是没有针对性的，而是采用广播方式发送。也就是说，当它要向某节点发送数据时，不是直接把数据发送到目的节点，而是把数据包发送到与集线器相连的所有节点。

正因如此，尽管集线器技术也在不断改进，但实质上就是加入了一些交换机(Switch)技术，发展到了今天的具有堆叠技术的堆叠式集线器，有的集线器还具有智能交换机功能。可以说集线器产品已在技术上向交换机技术进行了过渡，具备了一定的智能性和数据交换能力。但随着交换机价格的不断下降，仅有的价格优势已不再明显，集线器的市场越来越小，处于淘汰的边缘。尽管如此，集线器对于家庭或者小型企业来说，在经济上还是有一点诱惑力的，特别适合家庭几台机器的网络中或者中小型公司作为分支网络使用。

1.3.3 调制解调器

计算机内的信息是由 0 和 1 组成数字信号，而在电话线上传递的却只能是模拟电信号。于是，当两台计算机要通过电话线进行数据传输时，就需要一个设备负责数/模的转换。这



个数/模转换器就是调制解调器(Modem)。计算机在发送数据时,先由 Modem 把数字信号转换为相应的模拟信号,这个过程称为调制。经过调制的信号通过电话载波传送到另一台计算机之前,也要经由接收方的 Modem 负责把模拟信号还原为计算机能识别的数字信号,这个过程称为解调。正是通过这样一个调制与解调的数/模转换过程,从而实现了两台计算机之间的远程通信。

下面介绍 Modem 的类别。

一般来说,根据 Modem 的形态和安装方式,大致可以分为以下 5 类。

1. 外置式 Modem

外置式 Modem 放置于机箱外,通过串行通信口与主机连接。这种 Modem 方便灵巧、易于安装,闪烁的指示灯便于监视 Modem 的工作状况。但外置式 Modem 需要使用额外的电源与电缆。

2. 内置式 Modem

内置式 Modem 在安装时需要拆开机箱,并且要对中断和 COM 口进行设置,安装较为烦琐。这种 Modem 要占用主板上的扩展槽,但无须额外的电源与电缆,且价格比外置式 Modem 要便宜一些。

3. PCMCIA 插卡式 Modem

插卡式 Modem 主要用于笔记本电脑,体积纤巧。配合移动电话,可方便地实现移动办公。

4. 机架式 Modem

机架式 Modem 相当于把一组 Modem 集中于一个箱体或外壳里,并由统一的电源进行供电。机架式 Modem 主要用于 Internet/Intranet、电信局、校园网、金融机构等网络的中心机房。

5. USB 接口的调制解调器

USB 技术的出现,给计算机的外围设备提供更快的速度、更简单的连接方法。SHARK 公司率先推出了 USB 接口的 56Kbps 的调制解调器,这个只有呼机大小的调制解调器却给传统的串口调制解调器带来了挑战。只需将其接在主机的 USB 接口就可以,通常主机上有 2 个 USB 接口,而 USB 接口可连接 127 个设备。如果要连接多设备,还可购买 USB 的集线器。通常 USB 的显示器、打印机都可以当作 USB 的集线器,因为它们除了有连接主机的 USB 接口外还提供 1~2 个 USB 的接口。

除以上五种常见的 Modem 外,现在还有 ISDN 调制解调器和一种称为 Cable Modem 的调制解调器。另外,还有一种 ADSL 调制解调器。Cable Modem 利用有线电视的电缆进行信号传送,不但具有调制、解调功能,还集路由器、集线器、桥接器于一身,理论传输速度更可达 10Mbps 以上。通过 Cable Modem 上网,每个用户都有独立的 IP 地址,相当于拥有了一条个人专线。



1.3.4 交换机

以太网交换机是指带宽在100Mbps以下的以太网所用交换机。“快速以太网交换机”、“千兆以太网交换机”和“10千兆以太网交换机”其实也是以太网交换机，只不过它们所采用的协议标准或者传输介质不一样，当然其接口形式也不一样。

以太网交换机是最普遍和便宜的，它的档次比较齐全，应用领域也非常广泛，在大大小小的局域网都可以见到它们的踪影。以太网包括三种网络接口：RJ-45、BNC和AUI，所用的传输介质分别为双绞线、细同轴电缆和粗同轴电缆。不要以为一讲以太网就都是RJ-45接口的，只不过双绞线类型的RJ-45接口在网络设备中非常普遍而已。当然现在的交换机通常不可能全是BNC或AUI接口的，因为目前采用同轴电缆作为传输介质的网络已经很少见了，而一般是在RJ-45接口的基础上为了兼顾同轴电缆介质的网络连接，配上BNC或AUI接口。

交换机的工作原理如下。

(1) 交换机根据收到数据帧中的源MAC地址建立该地址同交换机端口的映射，并将其写入MAC地址表中。

(2) 交换机将数据帧中的目的MAC地址同已建立的MAC地址表进行比较，以决定由哪个端口进行转发。

(3) 如数据帧中的目的MAC地址不在MAC地址表中，则向所有端口转发。这一过程称为泛洪(flood)。

(4) 广播帧和组播帧，向所有的端口转发。

交换机对数据的转发有下列三种方式。

1. 直通式

直通方式的以太网交换机可以理解为在各端口间是纵横交叉的线路矩阵电话交换机。它在输入端口检测到一个数据包时，检查该包的包头，获取包的目的地址，启动内部的动态查找表转换成相应的输出端口，在输入与输出交叉处接通，把数据包直通到相应的端口，实现交换功能。由于不需要存储，延迟非常小、交换非常快，这是它的优点。它的缺点是，因为数据包内容并没有被以太网交换机保存下来，所以无法检查所传送的数据包是否有误，不能提供错误检测能力。由于没有缓存，不能将具有不同速率的输入/输出端口直接接通，而且容易丢包。

2. 存储转发

存储转发方式是计算机网络领域应用最为广泛的方式。它把输入端口的数据包检查，在对错误包处理后才取出数据包的目的地址，通过查找表转换成输出端口送出包。正因如此，存储转发方式在数据处理时延时大，这是它的不足，但是它可以对进入交换机的数据包进行错误检测，有效地改善网络性能。尤其重要的是它可以支持不同速度的端口间的转换，保持高速端口与低速端口间的协同工作。

3. 改进的直接交换

这是介于前两者之间的一种解决方案。它检查数据包的长度是否够64个字节，如果小于64字节，说明是假包，则丢弃该包；如果大于64字节，则发送该包。这种方式也不提供数据校验。它的数据处理速度比存储转发方式快，但比直通式慢。

1.3.5　路由器

路由器是连接因特网中各局域网、广域网的设备，它是会根据信道的情况自动选择和设定路由，以最佳路径，按前后顺序发送信号的设备。

目前路由器已经广泛应用于各行各业，各种不同档次的产品已经成为实现各种骨干网内部连接、骨干网间互联和骨干网与互联网互联互通业务的主力军。

路由就是指通过相互连接的网络把信息从"源地点"移动到"目标地点"的活动。一般来说，在路由过程中，信息至少会经过一个或多个中间节点。通常，人们会把路由和交换进行对比，这主要是因为在普通用户看来两者所实现的功能是完全一样的。其实，路由和交换之间的主要区别就是交换发生在OSI参考模型的第二层(数据链路层)，而路由发生在第三层，即网络层。这一区别决定了路由和交换在移动信息的过程中需要使用不同的控制信息，所以两者实现各自功能的方式是不同的。

早在40多年前就已经出现了对路由技术的讨论，但是直到20世纪80年代路由技术才逐渐进入商业化的应用。路由技术之所以在问世之初没有被广泛使用主要是因为80年代之前的网络结构都非常简单，路由技术没有用武之地。直到最近十几年，大规模的互联网络才逐渐流行起来，为路由技术的发展提供了良好的基础和平台。

路由器是互联网的主要节点设备。路由器通过路由决定数据的转发。转发策略称为路由选择，这也是路由器名称的由来。作为不同网络之间互相连接的枢纽，路由器系统构成了基于TCP/IP的国际互联网Internet的主体脉络，也可以说，路由器构成了Internet的骨架。它的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互联的质量。在当前我国网络基础建设和信息建设方兴未艾之际，探讨路由器在互联网络中的作用、地位及其发展方向，对于国内的网络技术研究、网络建设，以及明确网络市场上对于路由器和网络互联的各种似是而非的概念，都有重要的意义。

路由器是用于连接多个逻辑上分开的网络。所谓逻辑网络，是代表一个单独的网络或者一个子网。当数据从一个子网传输到另一个子网时，可通过路由器来完成。因此，路由器具有判断网络地址和选择路径的功能，它能在多网络互联环境中，建立灵活的连接，可用完全不同的数据分组和介质访问方法连接各种子网，路由器只接受源站或其他路由器的信息，属网络层的一种互联设备。它不关心各子网使用的硬件设备，但要求运行与网络层协议相一致的软件。路由器分本地路由器和远程路由器，本地路由器是用来连接网络传输介质的，如光纤、同轴电缆、双绞线；远程路由器是用来连接远程传输介质，并要求相应的设备，如电话线要配调制解调器，无线要通过无线接收机、发射机。其工作原理如下：

(1) 工作站A将工作站B的地址12.0.0.5连同数据信息以数据帧的形式发送给路由器1。



(2) 路由器1收到工作站A的数据帧后,先从报头中取出地址12.0.0.5,并根据路径表计算出发往工作站B的最佳路径R1→R2→R5→B;并将数据帧发往路由器2。

(3) 路由器2重复路由器1的工作,并将数据帧转发给路由器5。

(4) 路由器5同样取出目的地址,发现12.0.0.5就在该路由器所连接的网段上,于是将该数据帧直接交给工作站B。

(5) 工作站B收到工作站A的数据帧,一次通信过程宣告结束。

事实上,路由器除了上述的路由选择这一主要功能外,还具有网络流量控制功能。有的路由器仅支持单一协议,但大部分路由器可以支持多种协议的传输,即多协议路由器。由于每一种协议都有自己的规则,要在一个路由器中完成多种协议的算法,势必会降低路由器的性能。因此,我们以为,支持多协议的路由器性能相对较低。用户购买路由器时,需要根据自己的实际情况,选择自己需要的网络协议的路由器。

近年来出现了交换路由器产品,从本质上来说它不是什么新技术,而是为了提高通信能力,把交换机的原理组合到路由器中,使数据传输能力更快、更好。

从过滤网络流量的角度来看,路由器的作用与交换机和网桥非常相似。但是与工作在网络物理层、从物理上划分网段的交换机不同,路由器使用专门的软件协议从逻辑上对整个网络进行划分。例如,一台支持IP协议的路由器,可以把网络划分成多个子网段,只有指向特殊IP地址的网络流量才可以通过路由器。对于每一个接收到的数据包,路由器都会重新计算其校验值,并写入新的物理地址。因此,使用路由器转发和过滤数据的速度往往要比只查看数据包物理地址的交换机慢。但是,对于那些结构复杂的网络,使用路由器可以提高网络的整体效率。路由器的另外一个明显优势就是可以自动过滤网络广播。从总体上说,在网络中添加路由器的整个安装过程要比即插即用的交换机复杂很多。

互联网各种级别的网络中随处都可见到路由器,具体类型如下。

1. 接入路由器

接入路由器连接家庭或ISP内的小型企业客户。接入路由器已经开始不只是提供SLIP或PPP连接,还支持诸如PPTP和IPSec等虚拟私有网络协议。这些协议要能在每个端口上运行。诸如ADSL等技术将很快提高各家庭的可用带宽,这将进一步增加接入路由器的负担。由于这些趋势,接入路由器将来会支持许多异构和高速端口,并在各个端口能够运行多种协议,同时还要避开电话交换网。

2. 企业级路由器

企业或校园级路由器连接许多终端系统,其主要目标是以尽量便宜的方法实现尽可能多的端点互联,并且进一步要求支持不同的服务质量。许多现有的企业网络都是由Hub或网桥连接起来的以太网段。尽管这些设备价格便宜、易于安装、无须配置,但是它们不支持服务等级。相反,有路由器参与的网络能够将机器分成多个碰撞域,并因此能够控制一个网络的大小。此外,路由器还支持一定的服务等级,至少允许分成多个优先级别。但是路由器的每端口造价要贵些,并且在能够使用之前要进行大量的配置工作。因此,企业路由器的成败就在于是否提供大量端口且每端口的造价很低,是否容易配置,是否支持QoS。另外,还要求企业级路由器有效地支持广播和组播。企业网络还要处理历史遗留的各种LAN技

术，支持多种协议，包括 IP、IPX 和 Vine。它们还要支持防火墙、包过滤、大量的管理和安全策略以及 VLAN。

3. 骨干级路由器

骨干级路由器实现企业级网络的互联。对它的要求是速度和可靠性，而代价则处于次要地位。硬件可靠性可以采用电话交换网中使用的技术，如热备份、双电源、双数据通路等来获得。这些技术对所有骨干路由器而言差不多是标准的。骨干 IP 路由器的主要性能瓶颈是在转发表中查找某个路由所耗的时间。当收到一个包时，输入端口在转发表中查找该包的目的地址以确定其目的端口，当包越短或者当包要发往许多目的端口时，势必增加路由查找的代价。因此，将一些常访问的目的端口放到缓存中能够提高路由查找的效率。不管是输入缓冲还是输出缓冲路由器，都存在路由查找的瓶颈问题。除了性能瓶颈问题，路由器的稳定性也是一个常被忽视的问题。

4. 太比特路由器

在未来核心互联网使用的三种主要技术中，光纤和 DWDM 都已经是很成熟的并且是现成的。如果没有与现有的光纤技术和 DWDM 技术提供的原始带宽对应的路由器，新的网络基础设施将无法从根本上得到性能的改善。因此，开发高性能的骨干交换/路由器（太比特路由器）已经成为一项迫切的要求。太比特路由器技术现在还主要处于开发实验阶段。

5. 多 WAN 路由器

早在 2000 年，北京欣全向工程师在研究一种多链路（Multi-Homing）解决方案时发现，全部以太网协议的多 WAN 口设备在中国存在巨大的市场需求。伴随着欣全向产品研发成功，全国第一台双 WAN 路由器诞生于 2002 年，中国第一款双 WAN 宽带路由器被命名为 NuR8021。

双 WAN 路由器具有物理上的 2 个 WAN 口作为外网接入，这样内网计算机就可以经过双 WAN 路由器的负载均衡功能同时使用 2 条外网接入线路，大幅提高了网络带宽。当前双 WAN 路由器主要有“带宽汇聚”和“一网双线”的应用优势，这是传统单 WAN 路由器做不到的。

1.3.6　网桥

数据链路层互联的设备是网桥（Bridge），在网络互联中它起到数据接收、地址过滤与数据转发的作用，用来实现多个网络系统之间的数据交换。

网桥的基本特征如下：

- 网桥在数据链路层上实现局域网互联；
- 网桥能够互联两个采用不同数据链路层协议、不同传输介质与不同传输速率的网络；
- 网桥以接收、存储、地址过滤与转发的方式实现互联的网络之间的通信；
- 网桥需要互联的网络在数据链路层以上采用相同的协议；



- 网桥可以分隔两个网络之间的广播通信量，有利于改善互联网络的性能与安全性。

网桥像一个聪明的中继器。中继器从一个网络电缆里接收信号，放大它们，将其送入下一个电缆。相比较而言，网桥对从关卡上传下来的信息更敏锐一些。

网桥将两个相似的网络连接起来，并对网络数据的流通进行管理。它工作于数据链路层，不但能扩展网络的距离或范围，而且可提高网络的性能、可靠性和安全性。

网络1和网络2通过网桥连接后，网桥接收网络1发送的数据包，检查数据包中的地址，如果地址属于网络1，它就将其放弃；相反，如果是网络2的地址，它就继续发送给网络2。这样可利用网桥隔离信息，将网络划分成多个网段，隔离出安全网段，防止其他网段内的用户非法访问。由于网络的分段，各个网段相对独立，一个网段的故障不会影响到另一个网段的运行。

网桥可以是专门硬件设备，也可以由计算机加装的网桥软件来实现，这时计算机上会安装多个网络适配器(网卡)。

网桥的功能在延长网络跨度上类似于中继器，然而它能提供智能化连接服务，即根据帧的终点地址处于哪一网段来进行转发和滤除。网桥对站点所处网段的了解是靠“自学习”实现的。

当使用网桥连接两段LAN时，网桥对来自网段1的MAC帧，首先要检查其终点地址。如果该帧是发往网段1上某一站的，网桥则不将帧转发到网段2，而将其滤除；如果该帧是发往网段2上某一站的，网桥则将它转发到网段2。这表明，如果LAN1和LAN2上各有一对用户在本网段上同时进行通信，显然是可以实现的。因为网桥起到了隔离作用。可以看出，网桥在一定条件下具有增加网络带宽的作用。

网桥的存储和转发功能与中继器相比，其优点如下：

- 使用网桥进行互联克服了物理限制，这意味着构成LAN的数据站总数和网段数很容易扩充。
- 网桥纳入存储和转发功能可使其适应于连接使用不同MAC协议的两个LAN，因而构成一个不同LAN混连在一起的混合网络环境。
- 网桥的中继功能仅仅依赖于MAC帧的地址，因而对高层协议完全透明。
- 网桥将一个较大的LAN分成段，有利于改善可靠性、可用性和安全性。

网桥的主要缺点是由于网桥在执行转发前先接收帧并进行缓冲，与中继器相比会引入更多时延。由于网桥不提供流量控制功能，因此在流量较大时有可能使其过载，从而造成帧的丢失。

1.3.7 网关

网关(Gateway)又称网间连接器、协议转换器。网关在传输层上以实现网络互联，是最复杂的网络互联设备，仅用于两个高层协议不同的网络互联。网关的结构也和路由器类似，不同的是网络互联层。网关，既可以用于广域网互联，也可以用于局域网互联。

网关是一种充当转换重任的计算机系统或设备。在使用不同的通信协议、数据格式或语言，甚至体系结构完全不同的两种系统之间，网关是一个翻译器。与网桥只是简单地传达信息不同，网关对收到的信息要重新打包，以适应目的系统的需求。同时，网关也可以提供

过滤和安全功能。大多数网关运行在 OSI 7 层协议的顶层,即应用层。

举个例子,从一个房间走到另一个房间,必然要经过一扇门。同样,从一个网络向另一个网络发送信息,也必须经过一道“关口”,这道关口就是网关。顾名思义,网关就是一个网络连接到另一个网络的“关口”。

在 OSI 中,网关有两种:一种是面向连接的网关;一种是无连接的网关。当两个子网之间有一定距离时,往往将一个网关分成两半,中间用一条链路连接起来,称为半网关。

按照不同的分类标准,网关也有很多种。TCP/IP 协议里的网关是最常用的,在这里所讲的“网关”均指 TCP/IP 协议下的网关。

网关实质上是一个网络通向其他网络的 IP 地址。比如有网络 A 和网络 B,网络 A 的 IP 地址范围为 192.168.1.1～192.168.1.254,子网掩码为 255.255.255.0;网络 B 的 IP 地址范围为 192.168.2.1～192.168.2.254,子网掩码为 255.255.255.0。在没有路由器的情况下,两个网络之间是不能进行 TCP/IP 通信的,即使是两个网络连接在同一台交换机上,TCP/IP 协议也会根据子网掩码(255.255.255.0)判定两个网络中的主机处在不同的网络里。而要实现这两个网络之间的通信,则必须通过网关。如果网络 A 中的主机发现数据包的目的主机不在本地网络中,就把数据包转发给它自己的网关,再由网关转发给网络 B 的网关,网络 B 的网关再转发给网络 B 的某个主机。网络 B 向网络 A 转发数据包的过程则与此相反。

所以说,只有设置好网关的 IP 地址,TCP/IP 协议才能实现不同网络之间的相互通信。那么,这个 IP 地址是哪台机器的 IP 地址呢? 网关的 IP 地址是具有路由功能的设备的 IP 地址,具有路由功能的设备有路由器、启用了路由协议的服务器、代理服务器。

在和 Novell NetWare 网络交互操作的上下文中,网关在 Windows 网络中使用的服务器信息块 (SMB) 协议以及 NetWare 网络使用的 NetWare 核心协议 (NCP) 之间起着桥梁的作用。网关也被称为 IP 路由器。

如果搞清了什么是网关,默认网关也就好理解了。就好像一个房间可以有多扇门一样,一台主机可以有多个网关。默认网关的意思是一台主机如果找不到可用的网关,就把数据包发给默认指定的网关,由这个网关来处理数据包。现在主机使用的网关,一般指的是默认网关。

目前常见的网关类型如下。

1. 信令网关

信令网关主要完成 7 号信令网与 IP 网之间信令消息的中继。在 3G 初期,对于完成接入侧到核心网交换之间的消息的转接(3G 之间的 RANAP 消息,3G 与 2G 之间的 BSSAP 消息),另外还能完成 2G 的 MSC/GMSC 与软交换机之间 ISUP 消息的转接。

2. 中继网关

中继网关又叫 IP 网关,同时满足电信运营商和企业需求的 VoIP 设备。中继网关(IP 网关)基于中继板和媒体网关板建构,单板最多可以提供 128 路媒体转换、两个以太网口,机框采用业界领先的 CPCI 标准,扩容方便,具有高稳定性、高可靠性、高密度、容量大等特点。



3. 接入网关

接入网关是基于 IP 的语音/传真业务的媒体接入网关，提供高效、高质量的语音服务，为运营商、企业、小区、住宅用户等提供 VoIP 解决方案。

4. 协议网关

协议网关通常在使用不同协议的网络区域间做协议转换。这一转换过程可以发生在 OSI 参考模型的第 2 层、第 3 层或 2、3 层之间。但是有两种协议网关不提供转换的功能：安全网关和管道。由于两个互联的网络区域的逻辑差异，安全网关是两个技术上相似的网络区域间的必要中介，如私有广域网和公有的因特网。

5. 应用网关

应用网关是在使用不同数据格式间翻译数据的系统。典型的应用网关接收一种格式的输入，将之翻译，然后以新的格式发送。输入和输出接口可以是分立的，也可以使用同一网络连接。

应用网关也可以用于将局域网客户机与外部数据源相连，这种网关为本地主机提供了与远程交互式应用的连接。将应用的逻辑和执行代码置于局域网中，客户端避免了低带宽、高延迟的广域网的缺点，这就使得客户端的响应时间更短。应用网关将请求发送给相应的计算机，获取数据，如果需要就把数据格式转换成客户机所要求的格式。

6. 安全网关

安全网关是各种技术有趣的融合，具有重要且独特的保护作用，其范围从协议级向十分复杂的应用级过滤。

1.4 IP 网络基础

IP 是英文 Internet Protocol 的缩写，是为计算机网络相互连接而设计的协议。在因特网中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。有了 IP 协议，因特网才得以迅速发展成为世界上最大的、开放的计算机通信网络。

通俗地讲，IP 地址也可以称为互联网地址，是用来唯一标识互联网上计算机的逻辑地址。每台联网计算机都依靠 IP 地址来标识自己。

各个厂家生产的网络系统和设备，如以太网、分组交换网等，它们相互之间不能互通，主要原因是它们所传送数据的基本单元的格式不同。IP 协议实际上是一套由软件程序组成的协议软件，它把各种不同帧统一转换成“IP 数据包”格式，使各种计算机都能在因特网上实现互通。

数据包是分组交换的一种形式，就是把所传送的数据分段打成“包”，再传送出去。每个数据包都有报头和报文两部分，报头中有目的地址等内容，使每个数据包不经过同样的路径都能准确地到达目的地。在目的地重新组合还原成原来发送的数据。

IP 协议中还有一个非常重要的内容，就是给因特网上的每台计算机都规定了一个唯一的地址，叫做“IP 地址”。由于有这种唯一的 IP 地址，才保证了用户在联网的计算机上操作时，能够方便地从千千万万台计算机中选出自己所需的对象来。

1.4.1　IPv4

IP 地址就是给每个连接在 Internet 上的主机分配的一个 32bit 地址。按照 TCP/IP 协议规定，IP 地址用二进制数来表示，每个 IP 地址长 32bit，就是 4 个字节。例如，一个采用二进制数形式的 IP 地址是 00001010000000000000000000000001，这么长的地址使用起来非常麻烦。为了方便使用，IP 地址经常写成十进制数的形式，中间使用符号“.”分开不同的字节。

1. 基本地址格式

现在的 IP 网络使用 32 位地址，以点分十进制数表示，如 192.168.0.1。地址格式为：IP 地址＝网络地址＋子网地址＋主机地址。

网络地址是因特网协会的 ICANN 分配的，下有负责北美地区的 InterNIC、负责欧洲地区的 RIPENIC 和负责亚太地区的 APNIC，目的是保证网络地址的全球唯一性。主机地址是由各个网络的系统管理员分配。因此，网络地址的唯一性与网络内主机地址的唯一性确保了 IP 地址的全球唯一性。

2. 公共地址与私用地址

根据用途和安全性级别的不同，IP 地址还可以大致分为两类：公共地址和私有地址。公用地址在 Internet 中使用，可以在 Internet 中随意访问。私有地址只能在内部网络中使用，只有通过代理服务器才能与 Internet 通信。

3. IP 地址的分类

IP 地址分为五类：A 类保留给政府机构，B 类分配给中等规模的公司，C 类分配给任何需要的人，D 类用于组播，E 类用于实验。各类可容纳的地址数目不同。

- A 类地址。第 1 个字节为网络地址，其他 3 个字节为主机地址，地址范围为 1.0.0.1～126.255.255.254。A 类地址中既有私有地址也有保留地址，其中 10.×.×.×是私有地址，范围为 10.0.0.0～10.255.255.255；127.×.×.×是保留地址，用做循环测试。
- B 类地址。第 1 个字节和第 2 个字节为网络地址，其他 2 个字节为主机地址，地址范围为 128.0.0.1～191.255.255.254。B 类地址包括私有地址和保留地址，其中172.16.0.0～172.31.255.255 是私有地址，169.254.×.×是保留地址。
- C 类地址。第 1 个字节、第 2 个字节和第 3 个字节为网络地址，第 4 个字节为主机地址，地址范围为 192.0.0.1～223.255.255.254，其中 192.168.×.×是私有地址。
- D 类地址。不分网络地址和主机地址，地址范围为 224.0.0.1～239.255.255.254。
- E 类地址。不分网络地址和主机地址，地址范围为 240.0.0.1～255.255.255.254。



4. 特殊的 IP 地址

在 IP 地址空间中，有的 IP 地址是不能分配的，有的 IP 地址不能用在公网，有的 IP 地址只能在本机使用。诸如此类的特殊 IP 地址很多。

- 受限广播地址。广播通信是一对多的通信方式。若一个 IP 地址的二进制数全为 1，也就是 255.255.255.255，则这个地址用于定义整个互联网。如果想使 IP 数据报被整个 Internet 接收，就发送这个目的地址全为 1 的广播包，但这样会给整个互联网带来灾难性的负担。因此，网络上的所有路由器都阻止具有这种类型的分组被转发出去，使这样的广播仅限于本地网段。
- 直接广播地址。一个网络中的最后一个地址为直接广播地址，也就是 HostID 全为 1 的地址。主机使用这种地址把一个 IP 数据报发送到本地网段的所有设备上，路由器会转发这种数据报到特定网络上的所有主机。
- IP 地址是 0.0.0.0。若 IP 地址全为 0，也就是 0.0.0.0，则这个 IP 地址在 IP 数据报中只能用作源 IP 地址，这发生在当设备启动时但又不知道自己的 IP 地址情况下。
- NetID 为 0 的 IP 地址。当某个主机向同一网段上的其他主机发送报文时就可以使用这样的地址，分组也不会被路由器转发。例如，12.12.12.0/24 这个网络中的一台主机 12.12.12.2/24 在与同一网络中的另一台主机 12.12.12.8/24 通信时，目的地址可以是 0.0.0.8。
- 环回地址。127 网段的所有地址都称为环回地址，主要用来测试网络协议是否工作正常。例如，使用 ping 127.1.1.1 就可以测试本地 TCP/IP 协议是否已正确安装。另外一个用途是当客户进程用环回地址发送报文给位于同一台机器上的服务器进程，如在浏览器里输入 127.1.2.3，这样可以在排除网络路由的情况下测试 IIS 是否正常启动。
- 专用地址。IP 地址空间中，有一些 IP 地址被定义为专用地址，这样的地址不能为 Internet 的设备分配，只能在企业内部使用，因此也称为私有地址。若要在 Internet 上使用这样的地址，必须使用网络地址转换或者端口映射技术。

1.4.2 IPv6

IPv6 是 Internet Protocol Version 6 的缩写，也被称作下一代互联网协议，它是由 IETF 小组设计的用来替代现行 IPv4 协议的一种新的 IP 协议。

Internet 上的主机都有一个唯一的 IP 地址，IP 地址用一个 32bit 二进制数表示一个主机号码，但 32 位地址资源有限，已经不能满足需求了。因此 Internet 研究组织发布了新的主机标识方法，即 IPv6，用 128 位二进制数标识一个主机。在 RFC1884 中规定的标准语法建议把 IPv6 地址的 128 位写成 8 个 16 位的无符号整数，每个整数用四个十六进制位表示，中间用冒号分开，例如 3ffe:3201:1401:1280:c8ff:fe4d:db39:5420。这种 IP 标识方法具有如下特点：

(1) 扩展的寻址能力。IPv6 将 IP 地址长度从 32 位扩展到 128 位，支持更多级别的地址层次、更多的可寻址节点数以及更简单的地址自动配置。通过在组播地址中增加一个“范

围”域提高了多点传送路由的可扩展性。

(2) 简化的报头格式。一些 IPv4 报头字段被删除或变为了可选项，以减少包处理中例行处理的消耗并限制 IPv6 报头消耗的带宽。

(3) 对扩展报头和选项支持的改进。IP 报头选项编码方式的改变可以提高转发效率，使得对选项长度的限制更宽松，且提供了将来引入新的选项的更大的灵活性。

(4) 认证和加密能力。IPv6 中指定了支持认证、数据完整性和数据机密性的扩展功能。

1.4.3　代理 IP

代理 IP 就是代理服务器，其功能就是代理网络用户去取得网络信息。通常使用浏览器去连接 Internet 站点时，须送出 Request 请求来得到回答，然后对方再把信息传送回来。代理服务器是介于浏览器和 Web 服务器之间的一台服务器，有了它之后，浏览器不是直接到 Web 服务器去取回网页而是向代理服务器发出请求，Request 信号会先送到代理服务器，由代理服务器来取回浏览器所需要的信息并传送给浏览器。代理服务器是 Internet 链路级网关所提供的一种重要的安全功能，主要的功能如下：

- 突破自身 IP 访问限制，访问国外站点。
- 访问一些单位或团体的内部资源。
- 提高访问速度。

1.4.4　子网掩码

IP 地址是以网络号和主机号来标识网络上的主机的，只有在一个网络号下的计算机之间才能直接互通，不同网络号的计算机要通过网关才能互通。但这种划分方式在某些情况下显得不灵活。为此，IP 网络还允许划分成更小的网络，称为子网，这样就产生了子网掩码。子网掩码就是用来判断任意两个 IP 地址是否属于同一子网，只有在同一子网的计算机才能直接互通。

子网掩码中 255 对应的地址是网络地址，255 的二进制表示为 11111111。协议规定，掩码中前面部分连续的 1 对应的是网络地址，一般默认的子网掩码是 255.255.255.0，二进制表示为 11111111 11111111 11111111 00000000。如果把最后的 8 个 0 中拿出几位来设置成 1，使得连续的 1 增加，就会把这个地址的网络进一步划分得更小一些。

1.5　网络安全技术

计算机网络的安全问题很早就出现了，而且随着网络技术的发展和应用，网络安全问题表现得更为突出。据统计，全球约每 20 秒就发生一次计算机入侵事件，Internet 上的网络防火墙约 1/4 被突破，约 70%以上的网络主管人员报告因机密信息泄露而受到损失。这些问题突出表现在黑客攻击、恶性代码的网上扩散。



1.5.1 网络安全

1. 网络安全的含义

网络安全是一个关系到国家安全和主权、社会稳定、民族文化继承和发扬的重要问题。其重要性正随着全球信息化的步伐而变得越来越重要。网络安全是一门涉及计算机科学、网络技术、加密技术、信息安全技术、应用数学、数论和信息论等多种学科的综合性科学。

网络安全本质上就是网络信息的安全问题。从广义上讲，凡是涉及网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域，而且因各主体所处的角度不同对网络安全有不同的理解。网络安全指网络系统的硬件、软件及其系统中的数据受到保护，避免因偶然的或者恶意的原因而遭到破坏、更改、泄露，保证系统能连续、可靠、正常地运行，网络服务不中断。其特征是针对网络本身可能存在的安全问题，实施网络安全方案，以保证计算机网络自身的安全性为目标。

2. 网络安全问题

网络安全包括网络设备安全、网络系统安全、数据库安全等。安全问题主要表现在以下几个方面。

- 操作系统的安全问题。不论采用什么操作系统，在默认安装条件下都会存在一些安全问题，只有专门针对操作系统安全性进行严格的安全配置，才能达到一定的安全程度。
- CGI 程序代码的审计。如果是通用的 CGI 问题，防范起来还稍微容易一些，但是对于网站或软件供应商专门开发的一些 CGI 程序，很多存在严重的 CGI 问题。
- 拒绝服务攻击。随着电子商务的兴起，对网站实时性要求越来越高，拒绝服务攻击(Denial of Service，DoS)或分布式拒绝服务攻击(Distributed Denial-of-Service，DDoS)对网站威胁越来越大。
- 安全产品使用不当。每个网站都有一些网络安全设备，但由于安全产品本身问题或使用问题，这些产品并没有起到应有的作用。
- 缺少严格的网络安全管理制度。网络安全最重要的是在思想上高度重视，网站或局域网内部的安全需要用完备的安全制度来保障。建立和实施严密的计算机网络安全制度与策略是真正实现网络安全的基础。

3. 网络安全目标

目标的合理设置对网络安全意义重大。过低，达不到防护目的；过高，要求的人力和物力多，可能导致资源的浪费。网络安全的目标主要表现在以下方面。

- 可靠性。可靠性是网络安全的最基本要求之一。可靠性主要包括硬件可靠性、软件可靠性、人员可靠性、环境可靠性。
- 可用性。可用性是网络系统面向用户的安全性能，要求网络信息可被授权实体访问并按要求使用，包括对静态信息的可操作性和对动态信息的可见性。
- 保密性。保密性建立在可靠性和可用性基础上，保证网络信息只能由授权的用户读取。常用的信息保密技术有防侦听、信息加密和物理保密。

- 完整性。完整性要求网络信息未经授权不能进行修改，网络信息在存储或传输过程中要保持不被偶然或蓄意地删除、修改、伪造等，防止网络信息被破坏和丢失。

4. 网络安全服务

为了保证网络或数据传输足够安全，一个安全的计算机网络应能够提供如下服务。

- 实体认证。这是防止主动攻击的重要防御措施，对保障开放系统环境中各种信息的安全意义重大。认证就是识别和证实。识别是辨别一个实体的身份，证实是证明实体身份的真实性。OSI 环境提供了实体认证和信源认证的安全服务。
- 访问控制。访问控制指控制与限定网络用户对主机、应用与网络服务的访问。这种服务不仅可以提供单个用户，也可以提供给用户组中的所有用户。常用的访问控制服务是通过用户的身份确认与访问权限设置来确定用户身份的合法性，以及对主机、应用或服务访问的合法性。
- 数据保密性。其目的是保护网络中系统之间交换的数据，防止因数据被截获而造成的泄密。数据保密性又分为信息保密、选择数据段保密和业务流保密等。
- 数据完整性。这是针对非法地篡改信息、文件和业务流设置的防范措施，以保证资源可获得性。数据完整性又分为连接完整性、无连接完整性、选择数据段有连接完整性与选择数据段无连接完整性。
- 防抵赖。这是针对对方进行抵赖的防范措施，可用来证实发生过操作。防抵赖又分为对发送防抵赖和对接收防抵赖。
- 审计与监控。这是提高安全性的重要手段。它不仅能够识别谁访问了系统，还能指出系统如何被访问。因此，除使用一般的网管软件和系统监控管理系统外，还应使用目前较为成熟的网络监控设备或实时入侵检测和漏洞扫描设备。

5. 网络安全特征

一个安全的计算机网络应当包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等，应具有如下特征：

- 保密性，即信息不泄露给非授权用户、实体或过程。
- 完整性，即数据未授权不能进行改变的特性，指信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
- 可用性，即可被授权实体访问并按需使用的特性，需要时能存取所需的信息。
- 可控性，即对信息传播和内容具有控制能力。

6. 网络安全体系

构建一个健全的网络安全体系，需要对网络安全风险进行全面评估，并制定合理的安全策略，采取有效的安全措施，才能从根本上保证网络的安全。

1.5.2　数据保密技术

根据密钥类型不同可将现代密码技术分为两类：一类是对称加密（秘密钥匙加密）系



统；另一类是非对称加密(公开密钥加密)系统。

对称加密系统是加密和解密均采用同一把秘密钥匙，而且通信双方都必须获得这把钥匙，并保持钥匙的秘密。

对称密码系统的安全性依赖于以下两个因素。第一，加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的；第二，加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性，因此，我们没有必要确保算法的秘密性，而需要保证密钥的秘密性。对称加密系统的算法实现速度极快，从 AES 候选算法的测试结果看，软件实现的速度都达到了每秒数兆或数十兆比特。对称密码系统的这些特点使其有着广泛的应用。因为算法不需要保密，所以制造商可以开发出低成本的芯片以实现数据加密。这些芯片有着广泛的应用，适合于大规模生产。

对称加密系统最大的问题是密钥的分发和管理非常复杂、代价高昂。例如，对于具有 n 个用户的网络，需要 $n(n-1)/2$ 个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大、分布很广时，密钥的分配和保存就成了大问题。对称加密算法的另一个缺点是不能实现数字签名。

公开密钥加密系统采用的加密钥匙(公钥)和解密钥匙(私钥)是不同的。由于加密钥匙是公开的，密钥的分配和管理就很简单。例如，对于具有 n 个用户的网络，仅需要 $2n$ 个密钥。公开密钥加密系统还能够很容易地实现数字签名。因此，最适合于电子商务应用需要。在实际应用中，公开密钥加密系统并没有完全取代对称加密系统，这是因为公开密钥加密系统是基于尖端的数学难题，计算非常复杂，它的安全性更高，但它实现速度却远赶不上对称加密系统。在实际应用中可利用二者的各自优点，采用对称加密系统加密文件，采用公开密钥加密系统加密“加密文件”的密钥(会话密钥)。这就是混合加密系统，它较好地解决了运算速度问题和密钥分配管理问题。因此，公钥密码体制通常被用来加密关键性的、核心的机密数据，而对称密码体制通常被用来加密大量的数据。

1. 对称密钥密码技术

对称加密系统最著名的是美国数据加密标准 DES、AES(高级加密标准)和欧洲数据加密标准 IDEA。

1977 年，美国国家标准局正式公布实施了美国的数据加密标准 DES，公开它的加密算法，并批准用于非机密单位和商业上的保密通信。随后，DES 成为全世界使用最广泛的加密标准。加密与解密的密钥和流程是完全相同的，区别仅仅是加密与解密使用的子密钥序列的施加顺序刚好相反。

但是，经过 20 多年的使用，已经发现 DES 很多不足之处，对 DES 的破解方法也日趋有效。AES 将会替代 DES 成为新一代加密标准。

2. 非对称密钥密码技术

自公钥加密问世以来，学者们提出了许多种公钥加密方法，它们的安全性都是基于复杂的数学难题。根据所基于的数学难题来分类，有以下三类系统目前被认为是安全和有效的：大整数因子分解系统(代表性的有 RSA)、椭圆曲线离散对数系统(ECC)和离散对数系统(代表性的有 DSA)。

当前最著名、应用最广泛的公钥系统 RSA 是由 Rivet、Shamir、Adelman 提出的(简称为 RSA 系统),它的安全性是基于大整数因子分解的困难性,而大整数因子分解问题是数学上的著名难题,至今没有有效的方法予以解决。因此,可以确保 RSA 算法的安全性。RSA 系统是公钥系统的最具有典型意义的方法,大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是 RSA 算法。

RSA 系统的优点主要在于原理简单,易于使用。但是,随着分解大整数方法的进步及完善、计算机速度的提高以及计算机网络的发展(可以使用成千上万台机器同时进行大整数分解),作为 RSA 加解密安全保障的大整数要求越来越大。为了保证 RSA 使用的安全性,其密钥的位数一直在增加。例如,目前一般认为 RSA 需要 1024 位以上的字长才有安全保障。但是,密钥长度的增加导致了其加解密的速度大为降低,硬件实现也变得越来越难以忍受,这对使用 RSA 的应用带来了很重的负担,对进行大量安全交易的电子商务更是如此,从而使得其应用范围越来越受到制约。

DSA(Data Signature Algorithm)是基于离散对数问题的数字签名标准,它仅提供数字签名,不提供数据加密功能。

1.5.3　身份认证

用户身份认证是安全系统的第一道防线,目的是防止非法用户访问系统,其方法是由系统提供一定的方式让用户标识自己的名字或身份。每次用户要求进入系统时,由系统进行核对,通过鉴定后才提供机器使用权。

获得上机权的用户若要使用数据库,数据库管理系统还要进行用户标识和鉴定。用户标识和鉴定的方法有很多种,而且在一个系统中往往是多种方法并举,以获得更强的安全性。常用的方法是用一个用户名或者用户标识号来标明用户身份。系统内部记录着所有合法用户的标识,系统鉴别此用户是否是合法用户,若是,则可以进入下一步的核实;若不是,则不能使用系统。

为了进一步核实用户,系统常常要求用户输入口令(Password)。为保密起见,用户在终端上输入的口令不显示在屏幕上。系统核对口令以鉴别用户身份。

通过用户名和口令来鉴定用户的方法简单易行,但用户名与口令容易被人窃取,因此用户身份认证还可以采用比较复杂的计算过程和函数来完成,而智能卡技术、数字签名技术和生理特征(如指纹、体温、声纹、视网膜纹等)认证技术的迅速发展也为具有更高安全要求的用户身份认证提供了实用可行的技术基础。

1.5.4　访问控制

在今天,高速发展的互联网已经深入到社会生活的各个方面。对个人而言,互联网已使人们的生活方式发生了翻天覆地的变化;对企业而言,互联网改变了企业传统的营销方式及其内部管理机制。但是,在享受信息的高度网络化带来的种种便利之时,还必须应对随之而来的信息安全方面的种种挑战。没有安全保障的网络可以说是一座空中楼阁,安全性已逐渐成为网络建设的第一要素。特别随着网络规模的逐渐增大,所储存的数据逐渐增多,使



用者会要求网络能够对不同来源、不同角色所提出的网络访问进行控制，以确保自己的资源不受到非法的访问与篡改，这就要用到访问控制机制。

访问控制是网络安全防范和保护的主要核心策略，它的主要任务是保证网络资源不被非法使用和访问。访问控制规定了主体对客体访问的限制，并在身份识别的基础上，根据身份对提出资源访问的请求加以控制。它是对信息系统资源进行保护的重要措施，也是计算机系统最重要和最基础的安全机制。

1.5.5 防火墙技术

防火墙(Firewall)是一道介于开放的、不安全的公共网与信息、资源汇集的内部网之间的屏障，由一个或一组系统组成。狭义的防火墙指安装了防火墙软件的主机或路由器系统；广义的防火墙还包括整个网络的安全策略和安全行为。防火墙技术是任何企业最基本的安全技术，包括包过滤技术、网络地址翻译和应用级代理。

1. 包过滤技术

包过滤技术(Packet Filtering)是在网络层依据系统的过滤规则，对数据包进行选择和过滤，这种规则又称为访问控制表(ACLs)。该技术通过检查数据流中的每个数据包的源地址、目标地址、源端口、目的端口及协议状态或它们的组合来确定是否允许该数据包通过。这种防火墙通常安装在路由器上。

一般而言，包过滤技术包括两种基本类型：无状态检查的包过滤和有状态检查的包过滤。其区别在于，后者通过记住防火墙的所有通信状态，并根据状态信息来过滤整个通信流，而不仅仅是包。另外，两者均被配置为只过滤最有用的数据域，包括协议类型、IP 地址、TCP/UDP 端口、分段口和源路由信息，但还是有许多方法可绕过包过滤器进入 Internet，这是因为：

- TCP 只能在第 0 个分段中被过滤。
- 特洛伊木马可以使用 NAT 来使包过滤器失效。
- 许多包过滤器允许 1024 以上的端口通过。

所以，“纯”包过滤器的防火墙不能完全保证内部网的安全，而必须与代理服务器和网络地址翻译结合起来才能解决问题。

2. 网络地址翻译

网络地址翻译(Network Address Translation，NAT)最初的设计目的是增加在专用网络中可使用的 IP 地址数，但现在则用于屏蔽内部主机。NAT 通过将专用网络中的专用 IP 地址转换成在 Internet 上使用的全球唯一的公共 IP 地址，实现对黑客有效地隐藏所有 TCP/IP 级的有关内部主机信息的功能，使外部主机无法探测到它们。

NAT 实质上是一个基本的代理：一个主机充当代理，代表内部所有主机发出请求，从而将内部主机的身份从公用网上隐藏起来了。

许多防火墙都支持不同类型的网络地址翻译。按普及程度和可用性顺序，NAT 防火墙最基本的翻译模式包括：

- 静态翻译(Static Translation),也称为端口转发(Port Forwarding)。在这种模式中,一个指定的内部网络源有一个从不改变的固定翻译表。为使内部主机建立与外部主机的连接需要使用静态NAT。
- 动态翻译(Dynamic Translation),也称为自动模式、隐藏模式或IP伪装。在这种模式中,为了隐藏内部主机的身份或扩展内部网的地址空间,一个大的Internet客户群共享单一一个或一组小的Internet IP地址。
- 负载平衡翻译(Load Balancing Translation)。在这种模式中,一个IP地址和端口被翻译为同等配置的多个服务器的一个集中处,这样一个公共地址可以为许多服务器服务。
- 网络冗余翻译(Network Redundancy Translation)。在这种模式中,多个Internet连接被附加在一个NAT防火墙上,从而防火墙根据负载和可用性对这些连接进行选择和使用。

由于NAT仅在传输层上实现,所以隐藏在TCP/IP通信中有效的数据信息可以传输到高层,并且可用来寻找在高层通信中的缺点或者用来与特洛伊木马通信。

3. 应用级代理

开发代理的最初目的是对Web进行缓存,减少冗余访问,但现在主要用于防火墙。代理服务器通过侦听网络内部客户的服务请求,检查并验证其合法性。若合法,它将像一台客户机一样向真正的服务器发出请求并取回所需信息,最后再转发给客户。对于内部客户而言,代理服务器好像原始的公共服务器;对于公共服务器而言,代理服务器好像原始的客户一样,亦即代理服务器充当了双重身份,并将内部系统与外界完全隔离开来,外面只能看到代理服务器,而看不到任何内部资源。

应用级代理中的请求重新生成的过程和代理位于内部网与外部网之间的事实提供了许多安全优点,同时也存在不少安全隐患。

- 代理隐藏了私有客户,不让它们暴露给外界。如同NAT,代理服务器防止外部主机对内部机器上服务的连接。但不便的是,客户必须使用代理才能工作,且它们是不能被设置为网络透明工作。
- 代理能阻断危险的URL。但因为Web站点可被轻易地根据它的IP地址或整个地址号来进行简单的寻址,所以阻断URL也容易被消除。
- 代理能在危险的内容如病毒和特洛伊木马等传送给客户之前过滤掉它们,但是代理无法保护操作系统。
- 代理能检查返回内容的一致性。但大多数一致性检查都是在发现有被利用的弱点后才有效。
- 代理能消除在网络之间的传输层路由。使用代理可使TCP/IP包不能真正在内部网和外部网之间传输,并且可以防止大多数的服务拒绝和利用软件弱点的攻击。但协议存在是因为没有好的代理服务,阻断路由功能通常使用得不充分。
- 代理提供了单点的访问、控制和日志记录功能。代理保证所有内容都通过单一点,此点成为检查网络数据的检查点。

另外,代理服务器在执行上还有缓存频繁访问数据以消除冗余访问、平衡内部多个服务



器负载的性能优化功能。但如果每个服务都要有代理,则易形成服务瓶颈。

虽然代理服务被认为是最安全的防火墙技术,但由于代理软件不能保护操作系统不受服务拒绝攻击,也不保护对在服务器上运行的其他服务的攻击,所以纯代理仍有许多安全问题,并且效率低下。因此,大多数实际的安全代理的实现产品都包括包过滤功能和网络翻译来形成一个完整的防火墙。

1.5.6 虚拟专用网

虚拟专用网(VPN)是专用网络的延伸,它包含了类似 Internet 的共享或公共网络链接。通过 VPN 可以以模拟点对点专用链接的方式通过共享或公共网络在两台计算机之间发送数据。虚拟专用联网是创建和配置虚拟专用网的行为。

虚拟专用网(VPN)被定义为通过一个公用网络(通常是因特网)建立一个临时的、安全的连接,是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。

虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接,并保证数据的安全传输。通过将数据流转移到低成本的网络上,一个企业的虚拟专用网解决方案将大幅度地减少用户花费在城域网和远程网络连接上的费用。同时,这将简化网络的设计和管理,加速连接新的用户和网站。另外,虚拟专用网还可以保护现有的网络投资。随着用户的商业服务不断发展,企业的虚拟专用网解决方案可以使用户将精力集中到自己的生意上,而不是网络上。虚拟专用网可用于不断增长的移动用户的全球因特网接入,以实现安全连接;可用于实现企业网站之间安全通信的虚拟专用线路,用于经济有效地连接到商业伙伴和用户的外联虚拟专用网。

虚拟专用网至少应能提供如下功能:

- 加密数据,以保证通过公网传输的信息即使被他人截获也不会泄露。
- 信息认证和身份认证,保证信息的完整性、合法性,并能鉴别用户的身份。
- 提供访问控制,不同的用户有不同的访问权限。

根据 VPN 所起的作用,可以将 VPN 分为如下三类。

(1) VPDN(Virtual Private Dial Network)。在远程用户或移动雇员和公司内部网之间的 VPN,称为 VPDN。实现过程如下:用户拨号 NSP(网络服务提供商)的网络访问服务器(Network Access Server,NAS),发出 PPP 连接请求,NAS 收到呼叫后,在用户和 NAS 之间建立 PPP 链路,然后,NAS 对用户进行身份验证,确定是合法用户,就启动 VPDN 功能,与公司总部内部连接,访问其内部资源。

(2) Intranet VPN。在公司远程分支机构的 LAN 和公司总部 LAN 之间的 VPN。通过 Internet 这一公共网络将公司在各地分支机构的 LAN 连到公司总部的 LAN,以便公司内部的资源共享、文件传递等,可节省 DDN 等专线所带来的高额费用。

(3) Extranet VPN。在供应商、商业合作伙伴的 LAN 和公司的 LAN 之间的 VPN。由于不同公司网络环境的差异性,该产品必须能兼容不同的操作平台和协议。由于用户的多样性,公司的网络管理员还应该设置特定的访问控制表(Access Control List,ACL),根据访问者的身份、网络地址等参数来确定相应的访问权限,开放部分资源而非全部资源给外联

网的用户。

1.5.7 计算机病毒

随着计算机应用日趋广泛，学生接触、利用网络的机会增多，通过提问让他们对习以为常的问题有更加清晰的认识，以便更好地应用防病毒技术。

1. 病毒的定义

按《中华人民共和国计算机信息系统安全保护条例》中的规定，计算机病毒指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据、影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

一般而言，病毒包括特洛伊木马、病毒、细菌和蠕虫等。特洛伊木马和病毒不能脱离某些特定的应用程序、应用工具或系统而独立存在；而细菌和蠕虫是完整的程序，操作系统可以调度和运行它们。而且除特洛伊木马外，其他三种形式的病毒都能够复制。

2. 病毒传染方式

病毒若想摧毁对方的计算机系统，必须获得计算机系统的控制权。病毒的传染途径有电磁波、有线电路、军用或民用设备或直接放毒等。具体传播介质有计算机网络、软硬磁盘和光盘等。根据传输过程中病毒是否被激活，病毒传染分为静态传染和动态传染。

静态传染是指由于用户使用了 COPY、DISKCOPY 等复制命令或类似操作，一个病毒连同其载体文件一起从一处被复制到另一处。这时，病毒的载体程序不变，被复制后的病毒不会引起其他文件感染。而动态传染是指一个静态病毒被加载进入内存变为动态病毒后，当其传染模块被激活时所发生的传染操作，这是一种主动传染方式。与动态传染相伴随的常常是病毒的发作，给用户制造麻烦的就是这种传染方式。

3. 病毒结构

计算机病毒是一种特殊的程序，它寄生在正常的、合法的程序中，并以各种方式潜伏下来，伺机进行感染和破坏。在这种情况下，称原先的那个正常的、合法的程序为病毒的宿主或宿主程序。病毒程序一般由以下部分组成：

- 初始化部分。它指随着病毒宿主程序的执行而进入内存并使病毒相对独立于宿主程序的部分。
- 传染部分。它指能使病毒代码连接于宿主程序之上的部分，由传染的判断条件和完成病毒与宿主程序连接的病毒传染主体部分组成。
- 破坏部分或表现部分。它主要指破坏被传染系统或者在被传染系统设备上表现特定的现象。病毒的破坏或表现部分是病毒程序的主体，它在一定程度上反映了病毒设计者的意图。

4. 病毒的分类

病毒从不同的角度有不同的分类。按危害性分为良性病毒和恶性病毒，按寄生方式分



为代替式病毒、链接式病毒、转储式病毒、填充式病毒和覆盖式病毒等。按病毒感染的途径，病毒分为三类：

- 引导型病毒。引导型病毒是藏匿在磁盘片或硬盘的第一个扇区。每次启动计算机时，在操作系统还没被加载之前就被加载到内存中，这个特性使得病毒完全控制DOS的各类中断，并且拥有更大的能力进行传染与破坏。这类病毒也称磁盘引导区病毒，如Michelangelo、Disk Killer等病毒。
- 文件型病毒。文件型病毒通常寄生在可执行文件中，如 *.COM、*.EXE等。当这些文件被执行时，病毒的程序就跟着被执行。这类病毒也称为可执行文件病毒、应用程序病毒或操作系统病毒。
- 复合型病毒。这类病毒兼具有引导型病毒和文件型病毒的特性。它们既可以传染 *.COM和*.EXE文件，也可以传染磁盘的引导区。由于这个特性，使得这种病毒具有相当程度的传染力。一旦发病，其破坏性相当大，如Flip等病毒。

5. 病毒感染原理

不同感染途径的病毒的感染机制也不相同，具体表现如下：

- 引导型病毒感染原理。引导型病毒通过执行启动计算机的动作作为感染的途径。一般正常软盘启动动作为开机、执行BIOS、读入BOOT程序执行和加载DOS。
- 文件型病毒感染原理。由于文件型病毒分为非常驻型与常驻型两类，所以其感染的方式也不同。对非常驻型病毒而言，只要一执行中毒的程序文件，病毒便立即寻找磁盘中尚未感染病毒的文件，若找到了便加以感染。一般而言，对于.COM型文件，病毒替换它的第一条指令。对于.EXE文件，病毒改变入口指针。而常驻型病毒必须常驻内存，才能达到感染其他文件的目的。每一个程序文件在执行时，都会调用INT 21H中断命令，所以病毒必须拦截INT 21H的调用，使其先通过病毒的程序，再去执行真正的INT 21H服务程序。
- 复合型病毒感染原理。就启动动作来说，假设以感染复合型病毒的磁盘启动，那么病毒便先潜入内存中，伺机感染其他未中毒的磁盘，而当DOS载入内存后，病毒再拦截INT 21H以达到感染文件的目的。

6. 病毒的网络威胁

目前，病毒对网络的威胁主要表现在：

- 工作站受到的威胁。病毒对网络工作站的攻击途径主要包括利用软盘读写进行传播、通过网络共享进行攻击、通过电子邮件系统进行攻击、通过FTP下载进行攻击和通过WWW浏览进行攻击。
- 服务器受到的威胁。网络操作系统一般都采用Windows NT/2000 Server和少量UNIX/Linux，而UNIX/Linux本身的计算机病毒的流行报告几乎很少。早期Windows NT系统对病毒有一定的免疫能力，但到目前为止感染Windows NT系统的病毒已有一定数量。
- Web站点受到的威胁。一般Web站点，用户访问量很大，目前能通过Web站点传播的病毒只有脚本蠕虫、一些恶意Java代码和ActiveX。



7. 宏病毒

Word 所编辑的文本分为两类，即文本文件（Document）和模板文件（Template）。二者的主要区别在于文本文件中包含了文本数据信息，如文字、字体、段落篇章格式、图像数据等。此外，还记录了其对应的模板文件名但不包括宏代码。模板中除了包含所有文本信息外，还包括可执行的宏语言程序，系统是通过模板来控制文本。为了说明宏病毒的传染原理，这里以文件建立、打开的基本流程为例介绍宏程序所起的作用。

建立一个新文本时，系统首先打开了一个通用的模板文件，如 NORMAL.DOT 等。该模板中存放了一些新文本的初始化程序，这时系统根据其模板执行相应的程序，执行顺序是由模板到系统，即首先查找是否有所需要的宏。如建立新文件对应的是 FileNew 宏，找到则执行，否则执行系统内部默认的宏命令。

Word 宏病毒几乎是唯一可跨越不同硬件平台而生存、传染和流行的一类病毒。与感染普通.EXE 或.COM 文件的病毒相比，Word 宏病毒具有隐蔽性强、传播迅速、危害严重、难以防治等特点。具体表现为：

- 对 Word 的运行破坏。不能正常打印、封闭或改变文件存储路径、将文件改名等。
- 对系统的破坏。Word Basic 语言能够调用系统命令，这将造成破坏。

为了有效防止 Word 系统被感染，可将常用的 Word 模板文件改为只读属性。当文件被感染后，应及时加以清除，以防其进一步扩散和复制。通常可采取以下措施：

- 手工杀毒。以 Word 为例，从“工具”菜单选取“宏”一项，进入“管理器”，选取标题为“宏”的一页，在“宏 有效范围”下拉列表框中打开要检查的文档。这时在上面的列表框中就会出现该文档模板中所含的宏，将不明来源的自动执行宏删除即可。
- 使用专业软件杀毒。目前杀毒软件公司都具备清除宏病毒的能力，当然也只能对已知的宏病毒进行检查和清除。对于新出现的病毒或病毒的变种则可能不能正常地清除，或者将会破坏文件的完整性，此时还是采取手工清理。

8. CIH 病毒

CIH 病毒属于文件型病毒，只感染 Windows 9x 下可执行文件。当受感染的.EXE 文件执行后，该病毒便驻留在内存中，并感染所接触到的其他 PE（Portable Executable）格式执行程序。

随着技术更新的频率越来越快，主板生产厂商使用 EPROM 来做 BIOS 的存储器，这是一种可擦写的 ROM。通常所说的 BIOS 升级就是借助特殊程序修改 ROM 中 BIOS 里的固化程序。采用了这种可擦写的 EPROM，虽然方便了用户及时对 BIOS 进行升级处理，但同时也给病毒带来了可乘之机。CIH 的破坏性在于它会攻击 BIOS，覆盖硬盘，进入 Windows 内核。

为防范 CIH 病毒对计算机主板的破坏，需采取一些针对性的措施。

- 修改系统时间，跳过病毒的发作日。
- 有些计算机系统主板具备 BIOS 写保护跳线，但一般设置均为开，可将其拨至关的位置，这样可以防止病毒向 BIOS 写入信息。



- 检查 CIH 病毒的方法可采用压缩并解压缩文件的方式。如果解压缩出现问题，多半可以肯定有 CIHV1.2 的存在，但用该方法不能判断 CIHV1.4 病毒。
- 用户不要轻易启动从电子邮件或从网站上下载的未知软件。
- 由于病毒将垃圾码写入硬盘，导致硬盘中的数据不能恢复时，务必将重要数据备份，以免造成损失。

1.5.8 常用反病毒技术

1. 反病毒技术分类

从研究的角度，反病毒技术主要分三类：

- 预防病毒技术。它通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。主要手段包括加密可执行程序、引导区保护、系统监控与读写控制等。
- 检测病毒技术。它是通过对计算机病毒的特征来进行判断的侦测技术，如自身校验、关键字等。
- 消除病毒技术。它通过对病毒的分析，杀除病毒并恢复源文件。

2. 常用反病毒技术

从具体实现技术的角度，常用的反病毒技术有：

- 病毒代码扫描法。将新发现的病毒加以分析后根据其特征编成病毒代码，加入病毒特征库中。每当执行杀毒程序时，便立刻扫描程序文件，并与病毒代码比对，便能检测到是否有病毒。病毒码扫描法速度快、效率高。大多数防毒软件均采用这种方式，但是无法检测到未知的新病毒以及变种病毒。
- 加总比对法(Check-sum)。根据每个程序的文件名称、大小、时间、日期及内容，加总为一个检查码，再将检查码附在程序后面，或是将所有检查码放在同一个资料库中，再利用 Check-sum 系统，追踪并记录每个程序的检查码是否遭更改，以判断是否中毒。这种技术可检测到各种病毒，但最大的缺点就是误判率高，且无法确认是哪种病毒感染的。
- 人工智能陷阱(Rule-based)。它是一种监测计算机行为的常驻式扫描技术。它将所有病毒所产生的行为归纳起来，一旦发现内存的程序有任何不当的行为，系统就会有所警觉，并告知用户。其优点是执行速度快、手续简便，且可以检测到各式病毒；其缺点是程序设计难，且不容易考虑周全。
- 软件模拟扫描法。它专门用来对付千面人病毒(Polymorphic/Mutation Virus)。千面人病毒在每次传染时，都以不同的随机数加密于每个中毒的文件中，传统病毒代码比对的方式根本就无法找到这种病毒。软件模拟技术则是成功地模拟 CPU 执行，在其设计的 DOS 虚拟机器(Virtual Machine)下模拟执行病毒的变体引擎解码程序，将多型体病毒解开，使其显露原本的面目，再加以扫描。
- VICE(Virus Instruction Code Emulation)先知扫描法。它是继软件模拟技术后的

一大突破。既然软件模拟可以建立一个保护模式下的DOS虚拟机器，模拟CPU动作并模拟执行程序以解开变体引擎病毒，应用类似的技术也可以用来分析一般程序检查可疑的病毒代码。因此，VICE将工程师用来判断程序是否有病毒代码存在的方法分析归纳成专家系统知识库，再利用软件工程的模拟技术(Software Emulation)假执行新的病毒，就可分析出新病毒代码以对付以后的病毒。

- 实时的I/O扫描(Realtime I/O Scan)。通过实时地对资料的输入/输出动作做病毒代码比对的动作，希望能够在病毒尚未被执行之前，就能够将其防堵下来。理论上，这样的实时扫描程序会影响到整体的资料传输速率，但是使用实时的I/O扫描，文件传送进来之后，就等于扫过了一次毒。
- 文件宏病毒陷阱(MacroTrapTM)。它结合了病毒代码比对与人工智慧陷阱技术，依病毒行为模式(Rule base)来检测已知及未知的宏病毒。其中，配合对象链接与嵌套(Object Linking and Embedding)技术，可将宏与文件分开，并可有效地将宏病毒彻底清除。
- 空中抓毒(Catch Virus on he fly TM)。在资料传输过程中经过的一个节点即一台计算机上设计一套防毒软件，把网络中所有可能带有病毒的信息进行扫描，接收从网络中送来的资料。把要扫描的资料在这台计算机中暂时储存起来，然后扫描储存的资料，并根据管理员的设定处理中毒的文件，最后把检查过或处理过的资料传送到它原来要传送的计算机上。
- 主动内核技术(ActiveK)。它是将已经开发的各种网络防病毒技术直接在源程序级就嵌入到操作系统或网络系统的内核中，实现网络防病毒产品与操作系统的无缝连接。这种技术可以保证网络防病毒模块从系统的底层内核与各种操作系统和应用环境密切协调，确保防毒操作不会伤及到操作系统内核，同时确保杀灭病毒的功效。

1.6　TCP/IP 测试

1.6.1　ping

这个命令用来检测一帧数据从当前主机传送到目的主机所需要的时间。当网络中出现故障时，用ping命令来预测故障和确定故障源是非常有效的。如果执行ping不成功，则可以检查一下网线是否连通、网卡配置是否正确、IP地址是否可用等；如果执行ping成功而网络仍无法使用，则可能是网络系统的软件配置有问题。

ping的命令格式为：

```
Usage: ping [ - t ] [ - a] [ - n count] [ - l size] [ - f] [ - i TTL] [ - v TOS]
            [ - r count] [ - s count] [[ - j host - list] | [ - k host - list]]
            [ - w timeout] target_name
```

该命令的常用参数及对应的功能如表1-2所示。



表 1-2　ping 命令的常用参数及对应的功能

参数名称	对应的功能	参数名称	对应的功能
-t	ping 通具体的主机	-l size	发一个缓冲区内容
-a	解析地址	-w timeout	时间限制
-n count	发送请求的数量		

要想使用 ping 命令，要依次选择【开始】→【运行】命令，在打开的【运行】对话框中输入 cmd，调出【命令提示符】窗口，如图 1-3 所示。然后在【命令提示符】窗口中输入 ping 127.0.0.1，这个命令可以验证本地计算机上安装的 TCP/IP 以及配置是否正确。

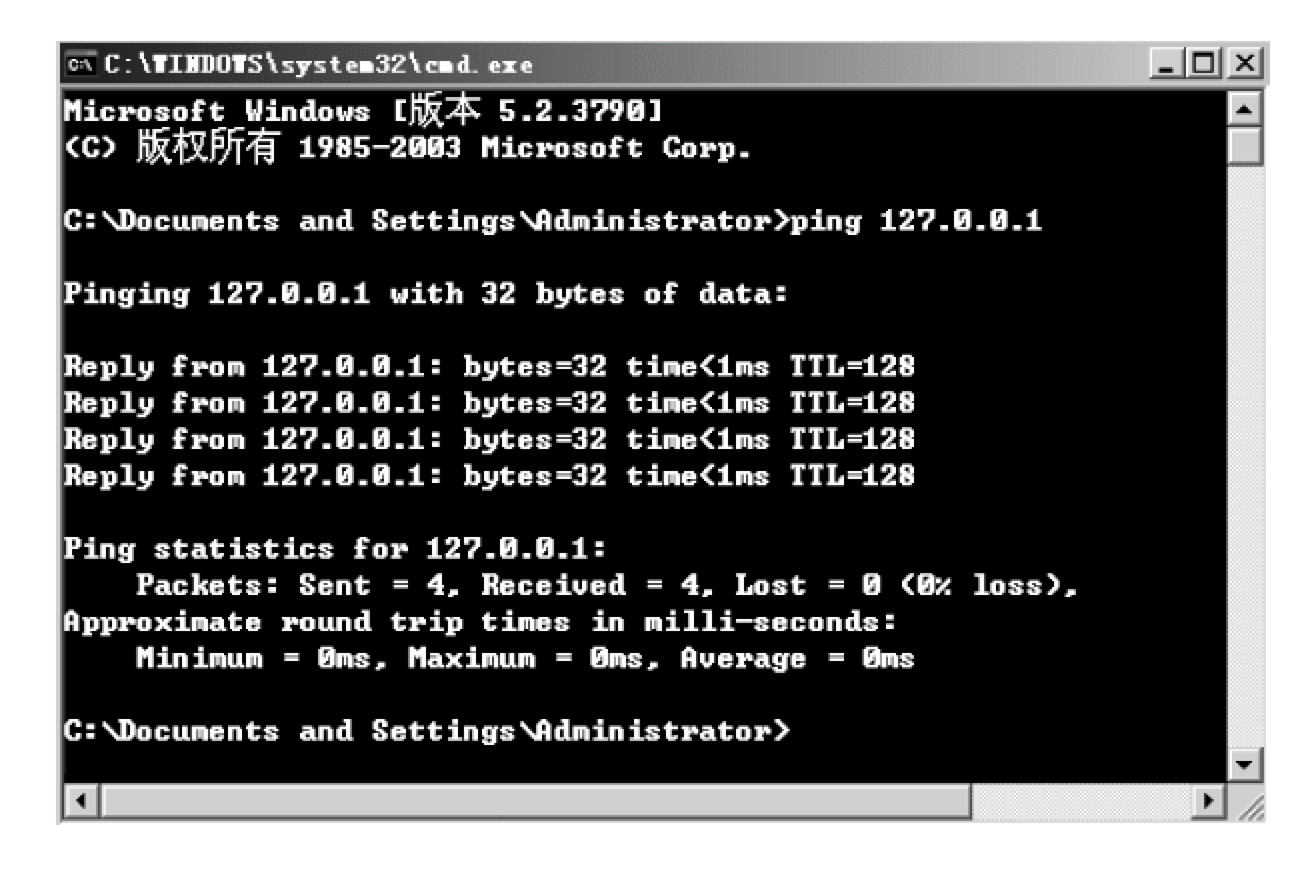


图 1-3　【命令提示符】窗口

1.6.2　tracert

这个命令的功能是判定数据包到达目的主机所经过的路径、显示数据包经过的中继节点清单和到达时间。还可以使用参数-d 决定是否解析主机名。命令格式为：

```
tracert [ - d] [ - h maximum_hops] [ - j host - list] [ - w timeout] target_name
```

该命令的常用参数及对应的功能如表 1-3 所示。

表 1-3　tracert 命令的常用参数及对应的功能

参数名称	对应的功能	参数名称	对应的功能
-d	不解析地址	-w timeout	每一跳的延时
-h maximum_hops	搜索 hops 的最大数目	-j host-list	排除列表中的路由

在图 1-3 所示的【命令提示符】窗口中输入 tracert www.sdjzu.edu.cn，即可跟踪连到该服务器的过程当中通过的路由。该命令的执行结果如下：

```
Tracing route to outwww.sdjzu.edu.cn [202.194.86.134]
over a maximum of 30 hops:
1     14 ms     14 ms     14 ms   119.164.128.1
2     15 ms     15 ms     15 ms   123.233.123.117
```



```
3     14 ms     15 ms     15 ms   60.217.40.61
4     14 ms     15 ms     15 ms   60.217.41.5
5     23 ms     23 ms     23 ms   219.158.18.221
6     23 ms     23 ms     23 ms   219.158.11.54
7    121 ms    122 ms    121 ms   219.158.34.198
8    123 ms    123 ms    122 ms   202.112.53.177
9    127 ms    128 ms     *       202.112.36.138
10    128 ms    128 ms    128 ms   202.112.61.26
```

1.6.3　netstat

这个命令可以帮助了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息，如采用的协议类型、当前主机与远端相连主机的 IP 地址以及它们之间的连接状态等。其命令格式如下：

```
netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

该命令的常用参数及对应的功能如表 1-4 所示。

表 1-4　netstat 命令的常用参数及对应的功能

参数名称	对应的功能
-a	显示所有连接和监听端口
-b	显示包含于创建每个连接或监听端口的可执行组件
-e	显示以太网统计信息。此选项可以与 -s 选项组合使用
-n	以数字形式显示地址和端口号
-o	显示与每个连接相关的所属进程 ID
-p proto	显示 proto 指定的协议的连接；proto 可以是下列协议之一：TCP、UDP、TCPv6 或 UDPv6
-r	显示路由表
-s	显示按协议统计信息
-v	为所有可执行组件创建连接或监听端口的组件
interval	暂停时间间隔

在图 1-3 所示的【命令提示符】窗口中输入 netstat -an，即可显示本机已经打开的所有连接和端口。该命令的执行结果如下：

```
Active Connections
Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:1464           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1498           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
TCP    0.0.0.0:9415           0.0.0.0:0              LISTENING
TCP    0.0.0.0:9701           0.0.0.0:0              LISTENING
TCP    0.0.0.0:10778          0.0.0.0:0              LISTENING
TCP    0.0.0.0:22692          0.0.0.0:0              LISTENING
```



```
TCP     0.0.0.0:25251          0.0.0.0:0             LISTENING
TCP     0.0.0.0:25274          0.0.0.0:0             LISTENING
TCP     119.164.133.229:1500   219.133.49.80:443     CLOSE_WAIT
TCP     119.164.133.229:2440   219.133.49.80:443     CLOSE_WAIT
TCP     119.164.133.229:3451   123.129.254.12:80     CLOSE_WAIT
TCP     119.164.133.229:3642   219.133.60.243:8000   CLOSE_WAIT
TCP     119.164.133.229:4822   110.75.161.35:16000   ESTABLISHED
```

1.6.4 ipconfig

ipconfig 是一个非常常用的命令，它可以查看本机的网络配置信息。其命令格式为：

```
ipconfig [/? | /all | /renew [adapter] | /release [adapter] |
          /flushdns | /displaydns | /registerdns |
          /showclassid adapter |
          /setclassid adapter [classid] ]
```

该命令的常用参数及对应的功能如表 1-5 所示。

表 1-5 ipconfig 命令的常用参数及对应的功能

参数名称	对应的功能	常用参数	对应的功能
/?	显示所有帮助信息	/release	解析指定网卡的 IP
/all	显示所有配置信息	/displaydns	显示 DNS 解析服务器

在图 1-3 所示的【命令提示符】窗口中输入 ipconfig /all，即可查看本机的所有网络配置信息。该命令的执行结果如下。

```
Windows IP Configuration
        Host Name . . . . . . . . . . . . : SL-200911061823
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8168C(P)/8111C(P) PCI-E G
igabit Ethernet NIC
        Physical Address. . . . . . . . . : 00-1E-EC-BA-C3-DA
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Autoconfiguration IP Address. . . : 169.254.202.2
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 169.254.202.2
Ethernet adapter 无线网络连接:
        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Broadcom 802.11g 网络适配器
        Physical Address. . . . . . . . . : 00-21-00-6A-6F-C5
PPP adapter ab:
        Connection-specific DNS Suffix  . :
```



```
Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . . . . . : 00 - 53 - 45 - 00 - 00 - 00
Dhcp Enabled. . . . . . . . . . . : No
IP Address. . . . . . . . . . . . : 119.164.133.229
Subnet Mask . . . . . . . . . . . : 255.255.255.255
Default Gateway . . . . . . . . . : 119.164.133.229
DNS Servers . . . . . . . . . . . : 202.102.128.68
NetBIOS over Tcpip. . . . . . . . : Disabled
```

1.7　疑难解答

1. 在 Windows 局域网内计算机之间互相不能 ping 通

不能 ping 通对方计算机的原因较多，建议主要从以下两个方面检查并加以解决：

(1) 物理连接的问题。计算机之间在物理上不可互访，可能是网卡没有安装好、集线设备有故障、网线有问题。在这种情况下使用 ping 命令时会提示超时。尝试 ping 局域网中的其他计算机，查看一下与其他计算机是否能够正常通信，以确定故障是发生在本地计算机还是发生在远程计算机。

(2) 对方计算机禁止 ping 动作。如果计算机禁止了 ICMP(Internet 控制协议)回显，或者安装了防火墙软件也会造成 ping 操作超时。建议在禁用对方计算机的网络防火墙后再使用 ping 命令进行测试。

2. IP 地址与系统硬件冲突

启动计算机时经常出现【系统探测到 IP 地址 10.115.223.198 与系统硬件地址 00:00:0E:63:E6:3D 冲突】提示框。有时连续出现好几个这样的提示框，如果不关闭这个提示框则其他的一切操作都将无法进行。

这种情况是由于本机 TCP/IP 协议中设置的 IP 地址与局域网中另外一台计算机或网络设备的 IP 地址发生冲突所致的。发生冲突的 IP 地址显然就是 10.115.223.198，系统硬件地址 00:00:0E:63:E6:3D 是另一台计算机网卡或其他网络设置的 MAC 地址。因为已经有其他网络设备的 MAC 地址 00:00:0E:63:E6:3D 绑定了 10.115.223.198 这个 IP 地址，所以本机网卡 MAC 地址若再次绑定这个 IP 地址则是无效的，因此会导致出现 IP 地址与系统硬件冲突的提示。

解决该问题的方法就是更改本机的 IP 地址，或者如果本机对 10.115.223.198 这个 IP 地址有合法使用权，那么应该更改另一台计算机的 IP 地址。

3. Windows Server 2003 系统网络连接收发数据都为 0

一台运行 Windows Server 2003 系统的计算机，安装好网卡驱动程序并设置好 IP 地址等参数后，系统托盘中显示网络已经连接。但在 ping 同一网络中其他计算机时提示不通，且连接状态中显示发送和接收数据均为 0。

这种情况首先应该 ping 本机 IP 地址，如果返回信息正常，则说明网络协议等方面的设



置没有问题，可能是硬件方面的原因。如果 ping 本机时提示不通，则说明网卡驱动程序或网络协议安装不正常，需要重新安装。确认是硬件方面的原因后，可以首先从更换 PCI 插槽着手来排除故障。其次考虑将网卡拿到其他计算机上测试看是否完好。如果都不行，则只能更换网卡。

4. ping 同一个域名得到不同 IP 地址

当使用 ping 命令检查某网站的域名时发现两次返回了不同的 IP 地址。

之所以出现这种情况，是因为该网站使用了 DNS 动态负载平衡技术。基于这种技术的站点，一个域名可以对应多个 IP 地址。假设网站域名为 www.sdjzu.edu.cn，那么在【命令提示符】窗口中使用 nslookup www.sdjzu.edu.cn 就能够查看该站点当前活动的 IP 地址信息。

5. 宽带路由器共享上网频繁掉线

局域网采用宽带路由器+ADSL Modem 的方式共享上网。路由器设置成自动连接模式，上网时总是出现瞬间掉线情况(大约每隔 20 分钟掉一次)。

从故障描述中分析，引发此故障的原因大致有两个方面：

- 一方面可能是路由器的设置存在问题。有的路由器在检测到连接在一定时间内处于空闲状态时自动断开连接，如果是这个问题可以设置为“永不断线”模式。
- 另一方面可能是 ISP 通过绑定 ADSL Modem 的 MAC 地址的方式限制用户使用路由方式上网，这种情况下可以将 ADSL Modem 的 MAC 地址“克隆”到宽带路由器中使用。

6. 使用宽带路由器无法上网

局域网计算机通过 ADSL 线路+宽带路由器的方式共享上网，将宽带路由器的 WAN 端口和 ADSL Modem 连接。按照路由器设置说明对路由器进行相关设置后无法上网。

该问题分析如下：能够 ping 通路由器只能说明路由器的 LAN 端口设置没有问题，而且计算机与路由器之间能够正常通信。故障原因可能处在 WAN 端口及 ADSL Modem 的设置问题上，建议从以下方面进行检查：

- 宽带路由器没有正确设置 WAN 口，建议仔细查阅说明书进行相关设置。
- 宽带路由器与 ADSL Modem 的连接不正确。通常情况下，路由器与 ADSL Modem 的连接应当使用直通线，检查线缆类型是否合适。
- 工作站网络设置错误。一般宽带路由器会自动分配 IP 地址，因此客户端只需设置为自动获取 IP 地址即可。用户不必设置 IP 地址或其他网络参数。

7. 无法登录 ADSL Modem 管理界面

局域网通过 ADSL Modem 拨号上网。由于最近经常掉线，因此想查看 ADSL Modem 管理界面中的日志。在登录管理界面时发现很难登录成功，只能在关闭 ADSL Modem 电源后重新开启才能顺利登录。

根据故障描述可以判断掉线现象可能是因为并发访问量太大导致 ADSL Modem 超负

荷运转造成的，不能登录 ADSL Modem 管理界面的故障也可能是因为这个原因。建议禁止用户使用 BT 下载等易产生较大数据流量的上网操作。另外，还需要检查局域网中所有计算机中是否有已知或未知的蠕虫病毒，这类病毒也极有可能使网络访问的速度变得极为缓慢，从而导致用户在访问 ADSL Modem 的管理页面时出现不正常的超长延时访问现象。

8. 如何使用 TCP/IP 的常用测试命令

要使用 TCP/IP 的常用测试命令，操作步骤如下：

(1) 依次选择【开始】→【程序】→【附件】→【命令提示符】命令，进入【命令提示符】窗口。

(2) 执行 ipconfig 命令检查 TCP/IP 通信协议是否已经正常启动。如果设置正确，窗口会提示当前的 IP 地址、子网掩码、默认网关等信息。用 ipconfig /all 命令来检查，则能提供更详细的信息。

(3) 执行 ping 127.0.0.1 命令，检查网卡与驱动程序是否运行正常。

(4) 执行 ping(本机的 IP 地址)命令，检查 IP 地址是否正常。

(5) 执行 ping (默认网关)命令，检查网关是否运行正常。

(6) 执行 ping www.sohu.com 命令，检查是否可以正常联网。

(7) 执行 ipconfig /release 命令和 ipconfig /renew 命令，释放和得到 IP 地址。

习　　题

1. 填空题

(1) 一个网络协议主要由语法、________及________三要素组成。

(2) TCP/IP 模型由低到高分别为________、________、________、________层次。

(3) TCP/IP 体系结构的传输层上定义的两个传输协议为________和________。

(4) 在 TCP/IP 层次模型的网络层中包括的协议主要有 IP、IMCP、________和________。

(5) 常用的 IP 地址有 A、B、C 三类，128.11.3.31 是一个________类地址，其网络标识为________，主机标识为________。

2. 选择题

(1) IP 地址的位数为(　　)位。

A. 32　　B. 48　　C. 128　　D. 64

(2) 以下 IP 地址中，属于 B 类地址的是(　　)。

A. 112.213.12.23　　B. 210.123.23.12

C. 23.123.213.23　　D. 156.123.32.12

(3) Intranet 技术主要由一系列的组件和技术构成，Intranet 的网络协议核心是(　　)。

A. ISP/SPX　　B. PPP　　C. TCP/IP　　D. SLIP

(4) TCP/IP 协议集的网间网层上的 RARP 子协议的功能是(　　)。

A. 用于传输 IP 数据报　　B. 实现物理地址到 IP 地址的映射

C. 实现 IP 地址到物理地址的映射　　D. 用于该层上控制信息产生



(5) 下列给出的协议中,属于TCP/IP协议结构的应用层是(　　)。

A. UDP　　B. IP　　C. TCP　　D. Telnet

(6) 在TCP/IP协议中,Telnet协议是在(　　)。

A. 网络接口层　　B. 网络互联层　　C. 传输层　　D. 应用层

(7) 下面(　　)不是Web工作的部分。

A. 客户机　　B. 服务器　　C. HTTP协议　　D. FTP协议

(8) TCP/IP协议应用层中HTTP协议与传输层进行交换数据是通过(　　)端口。

A. 80　　B. 110　　C. 21　　D. 28

(9) 如果一台主机的IP地址为192.168.0.10,子网掩码为2555.255.255.224,那么主机所在网络的网络号占IP地址的(　　)位。

A. 24　　B. 25　　C. 27　　D. 28

(10) TCP/IP网络协议主要在OSI模型的(　　)上操作。

A. 数据链路层、传输层、物理层　　B. 物理层、传输层、会话层

C. 网络层、传输层、数据链路层　　D. 网络层、传输层、会话层

(11) 在TCP/IP协议族中,UDP协议工作在(　　)。

A. 应用层　　B. 传输层　　C. 网络接口层　　D. 网络互联层

(12) 连接两个TCP/IP局域网要求(　　)硬件。

A. 网桥　　B. 路由器　　C. 集线器　　D. 以上都是

(13) (　　)协议负责将MAC地址转换成IP地址。

A. TCP　　B. ARP　　C. UDP　　D. RARP

(14) TCP/IP体系结构中的TCP和IP所提供的服务分别为(　　)。

A. 链路层服务和网络层服务　　B. 网络层服务和传输层服务

C. 传输层服务和应用层服务　　D. 传输层服务和网络层服务

(15) IP协议实现信息传递依据的是(　　)。

A. URL　　B. IP地址　　C. 域名系统　　D. 路由器

3. 思考题

(1) 什么网络命令可以用于确定本地主机是否能与另一台主机交换(发送与接收)数据报?

(2) 什么网络命令可以显示当前的TCP/IP配置的设置值?

(3) 请说出通过ping命令检测网络故障的典型次序,并说出其使用的命令格式。

第2章　DNS服务器配置与管理

本章要点

- DNS 服务的工作原理
- 创建和设置 DNS 区域
- 建立和管理 DNS 资源记录

在 Internet 上，多数用户喜欢使用有意义的名称（如 www. sohu. com）来定位诸如网络上的邮件服务器或 Web 服务器这样的计算机。有意义的名称更容易记住，但是计算机使用数字地址（IP 地址）在网络上通信。为了更方便地使用网络资源，需要提供一种方法，将用户有意义的计算机或服务名称映射为数字地址。域名系统就是最通用的一种方法。

2.1　了解 DNS 服务

DNS 是域名系统（Domain Name System）的缩写，是一种组织成域层次结构的计算机和网络服务命名系统。DNS 命名用于在 Internet 上为主机赋予有意义的名称，帮助用户记忆、识别、定位计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与此名称相关的其他信息，如 IP 地址。

2.1.1　DNS 服务概述

整个域名系统包括以下 4 个组成部分：

- DNS 域名称空间。指定用于组织名称的域的层次结构。
- 资源记录。将 DNS 域名映射到特定类型的资源信息，以供在名称空间中注册或解析名称时使用。
- DNS 服务器。存储和应答资源记录的名称查询。
- DNS 客户机。用来查询服务器，将名称解析为查询中指定的资源记录类型。

DNS 域名称空间是一种树状结构。目前 InterNIC 管理全世界的 IP 地址，也负责管理整个域结构。在 InterNIC 之下的 DNS 结构分为多个域，如图 2-1 中根域下的多个顶级域都归 InterNIC 管理。顶级域可以再细分为二级域，如图中 microsoft 为公司名称，而二级域



下面又可以再划分子域，如 example。最下面一层被称为主机名称，如 host-a。一般一台主机使用完整的名称来表示，如 host-a. example. microsoft. com。

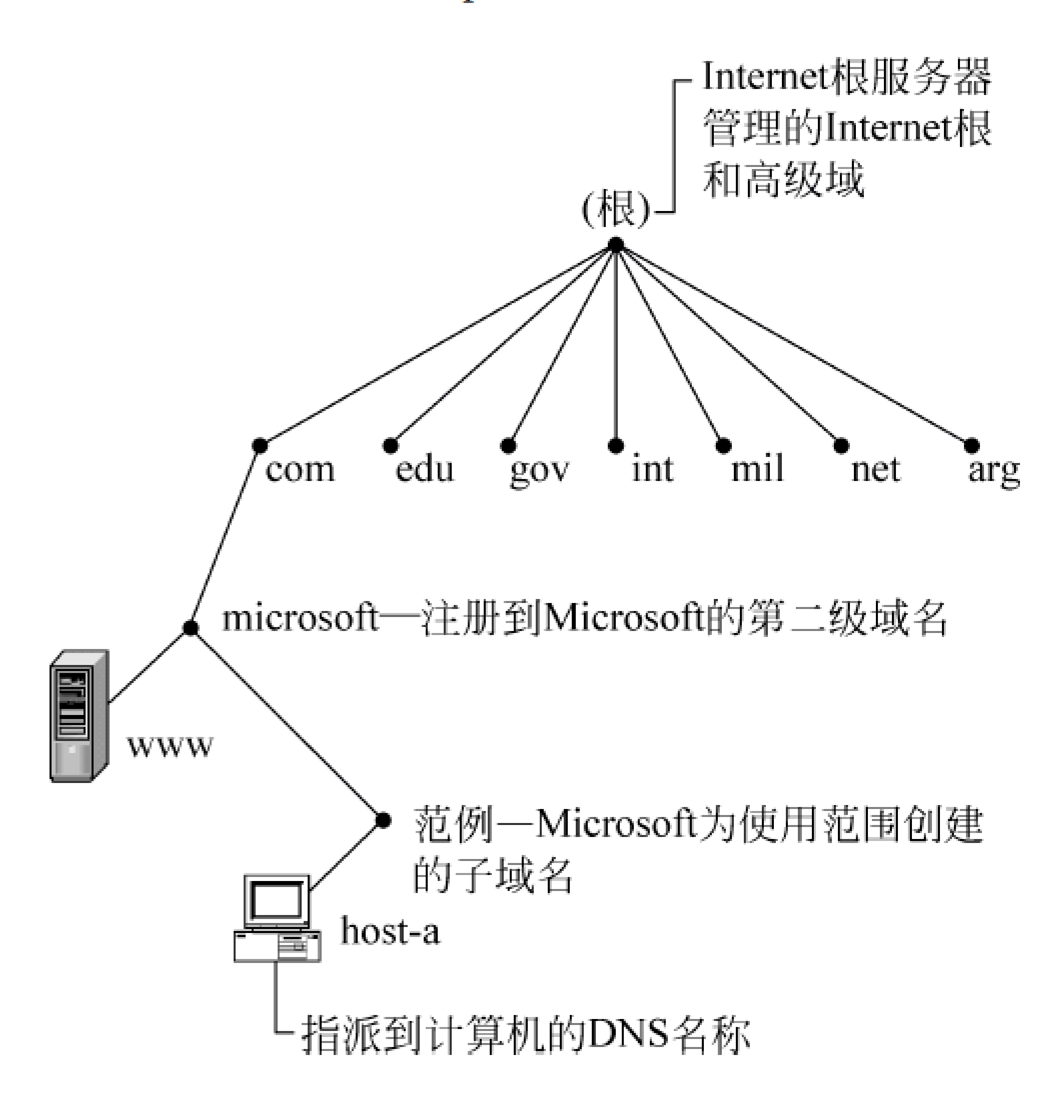


图 2-1　**域名称空间树状结构示意图**

2.1.2　DNS 服务的工作原理

当 DNS 客户机向 DNS 服务器提出查询请求时，每个查询信息都包括两部分信息：

- 一个指定的 DNS 域名，要求使用完整名称。
- 指定查询类型，既可以指定资源记录类型又可以指定查询操作的类型。

若指定的名称为一台计算机的完整域名 host-a. example. microsoft. com，指定的查询类型为主机（A）资源记录，可以理解为客户机询问服务器“有关主机名称为 host-a. example. microsoft. com 的计算机的 IP 地址记录吗”？当客户机收到服务器的回答信息时，它解读该信息，从中获得查询名称的 IP 地址。

DNS 的查询解析可以通过多种方式实现：客户机利用缓存中记录的以前的查询信息直接回答查询请求；DNS 服务器通过查询其他服务器获得查询信息并将它发送给客户机，这种查询方式称为递归查询；客户机通过 DNS 服务器提供的地址直接尝试向其他 DNS 服务器提出查询请求，这种查询方式称为迭代查询；当 DNS 客户机利用 IP 地址查询域名时，被称为反向查询。

当在客户机的浏览器中输入一个 DNS 域名，则客户机产生一个查询。如图 2-2 显示了查询域名为 host-b. example. microsoft. com 的计算机的过程。

（1）DNS 客户机利用本机的缓存信息进行解析，如果查询信息可以被解析，则完成查询。

（2）如果在本地无法获得查询信息，则客户机将查询请求发送给首选 DNS 服务器。当首选 DNS 服务器接到查询后，首先在首选服务器管理的区域的记录中查找，如果找到相应的记录，则利用此记录进行解析。





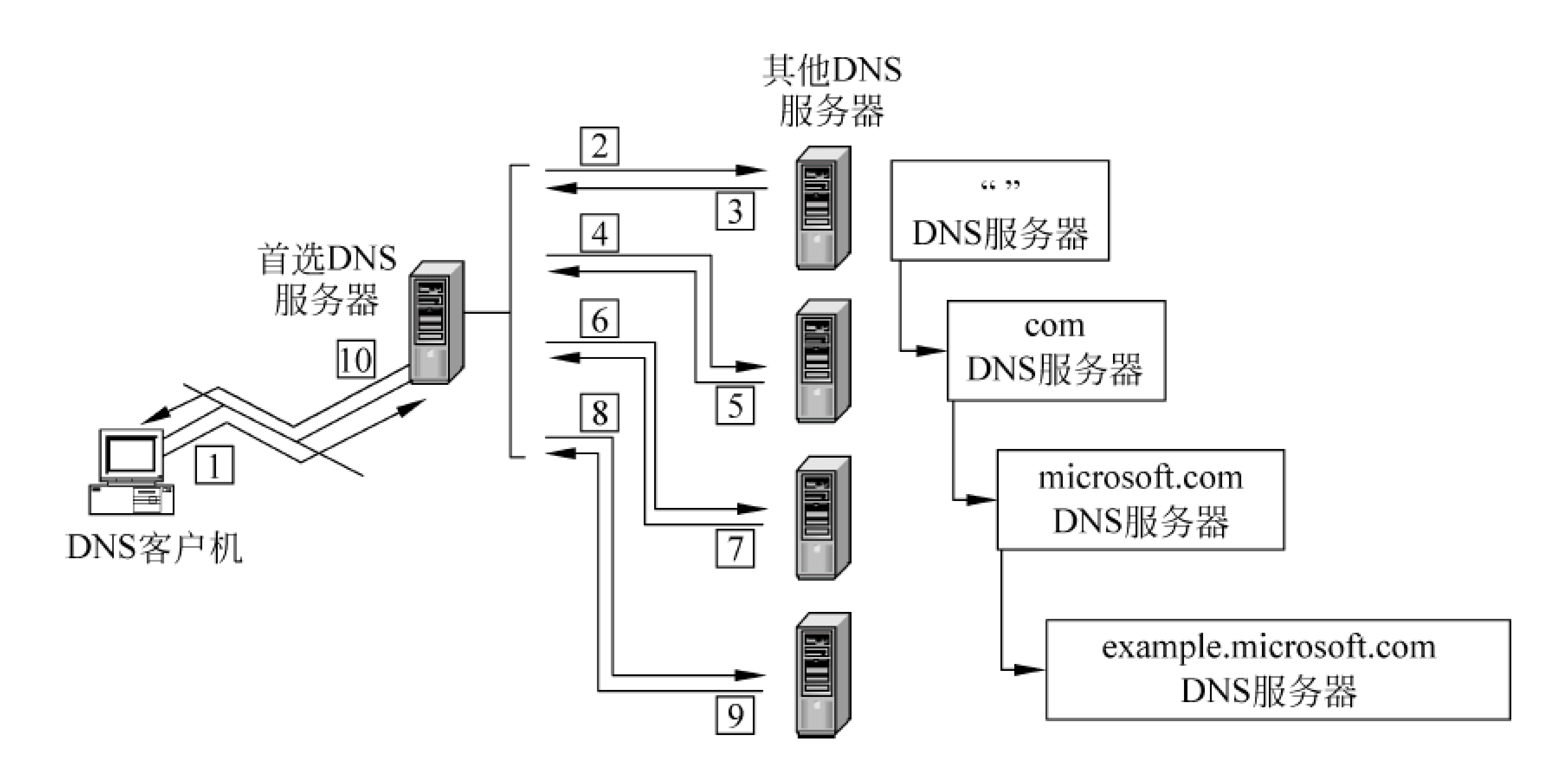


图 2-2　DNS查询的过程

(3) 如果在首选 DNS 服务器中仍无法查找到答案,则利用迭代查询进行名称的全面解析,这需要网络中的其他 DNS 服务器协助。默认情况下服务器支持迭代查询。

(4) 首选 DNS 服务器向根域名服务器发出查询请求,根域名服务器通过查询确定它属于哪个顶级域,即 com。

(5) 首选 DNS 服务器向 com 域的 DNS 服务器发起查询以获得 microsoft.com 的 DNS 服务器的地址。

(6) 首选 DNS 服务器以同样的方法从 microsoft.com 的 DNS 服务器获得 example.microsoft.com 的 DNS 服务器的地址。

(7) 首选 DNS 服务器与 example.microsoft.com 的 DNS 服务器进行通信,由于用户所要查询的域名包含在该服务器管理的区域中,它向首选 DNS 服务器发送一个回答,首选 DNS 服务器将这个回答转发给提出查询的客户机。到此查询过程结束。

2.2　DNS 服务器的安装

要使用 DNS 服务,就要安装 DNS 服务器。下面以 Windows Server 2003 为例来介绍。首先检查本地计算机是否已安装 DNS 服务组件:依次选择【开始】→【程序】→【管理工具】命令,此时如没有出现 DNS 子菜单,则需按以下步骤安装:

(1) 依次选择【开始】→【设置】→【控制面板】命令,打开【控制面板】窗口。

(2) 在【控制面板】窗口中,双击【添加或删除程序】快捷方式,打开【添加或删除程序】对话框。

(3) 在【添加或删除程序】对话框中,单击左边的【添加/删除 Windows 组件】按钮,打开如图 2-3 所示的【Windows 组件向导】对话框。

(4) 在其中的【组件】列表中,双击【网络服务】复选框,打开如图 2-4 所示的【网络服务】对话框。在其中选中【域名系统(DNS)】复选框,单击【确定】按钮。

(5) 在【Windows 组件向导】对话框中,单击【下一步】按钮,出现安装提示。在光驱中插入 Windows Server 2003 系统安装盘后,按提示完成安装。





图 2-3 【Windows 组件向导】对话框

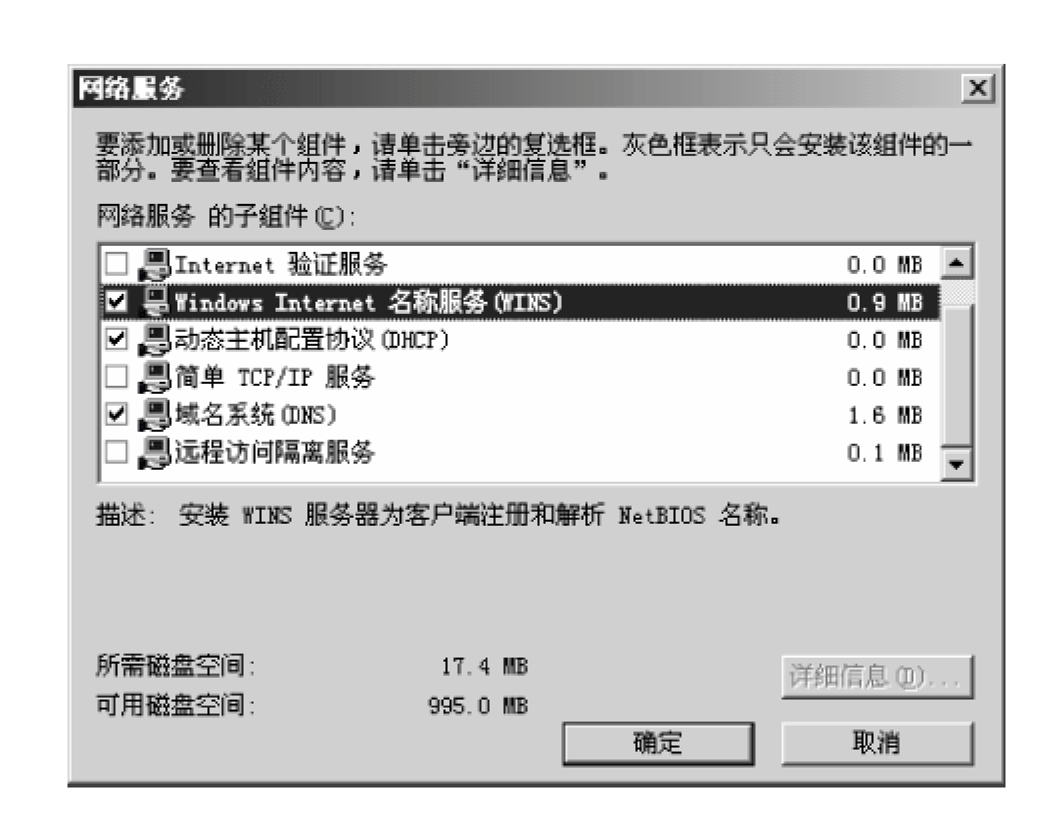


图 2-4 【网络服务】对话框

2.3 DNS 服务器级的管理

2.3.1 DNS 控制台

DNS 服务安装完成以后，会自动在【管理工具】菜单中增加一个 DNS 子菜单。依次选择【开始】→【程序】→【管理工具】→DNS 命令，打开如图 2-5 所示的 DNS 控制台窗口，即可对 DNS 服务进行配置管理。

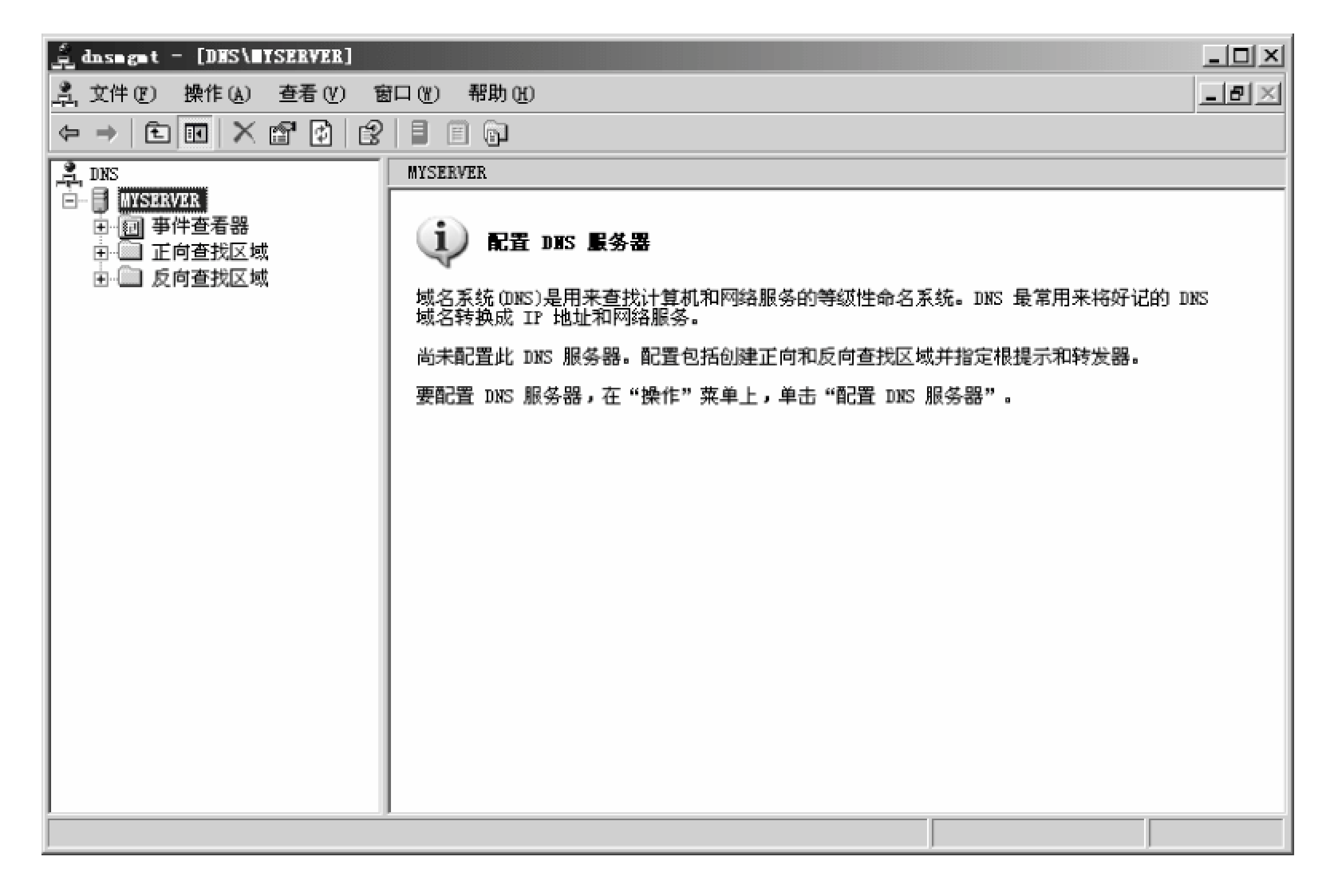


图 2-5 DNS 控制台窗口

安装 DNS 服务器后，系统自动将本机默认的 DNS 服务器添加到 DNS 控制台的目录树中。当然，还可将网上的其他 Windows 2003 DNS 服务器添加到控制台中进行管理。



2.3.2　DNS 服务器级的基本设置

在 DNS 控制台中，可以进行 DNS 服务器级的基本设置。在控制台目录树中，选择相应的 DNS 服务器，右击，从弹出的快捷菜单中选择【所有任务】命令，再从相应的下拉菜单中选择【开始】、【停止】、【暂停】或【重新启动】等命令，即可对整个 DNS 服务器进行相应的管理。

2.4　创建和设置 DNS 区域

DNS 名称空间可分成若干区域，区域存储有关一个或多个 DNS 域的名称信息。对于包括在区域中的每个 DNS 域名，该区域成为该域的有关信息的权威性信息源。设置 DNS 服务器，首要的任务就是建立 DNS 区域和域的树状结构。DNS 服务器以区域为单位来管理服务，区域是一个数据库，用来链接 DNS 名称和相关数据，如 IP 地址和网络服务。在 Internet 环境中一般用二级域名来命名，如 microsoft. com。

DNS 区域分为两类：一类是正向搜索区域，即域名到 IP 地址的数据库，用于提供将域名转换为 IP 地址服务；另一类是反向搜索区域，即 IP 地址到域名的数据库，用于提供将 IP 地址转换为域名的服务。这里先介绍正向搜索区域。

2.4.1　创建 DNS 正向搜索区域

创建 DNS 正向搜索区域的操作步骤如下：

(1) 在 DNS 控制台树中右击要配置的 DNS 服务器下面的【正向搜索区域】节点，从弹出的快捷菜单中选择【新建区域】命令，启动新建区域向导。

(2) 单击【下一步】按钮，打开如图 2-6 所示的【区域类型】对话框，选择区域类型。这里有 3 种区域类型，分别为主要区域、辅助区域和存根区域。

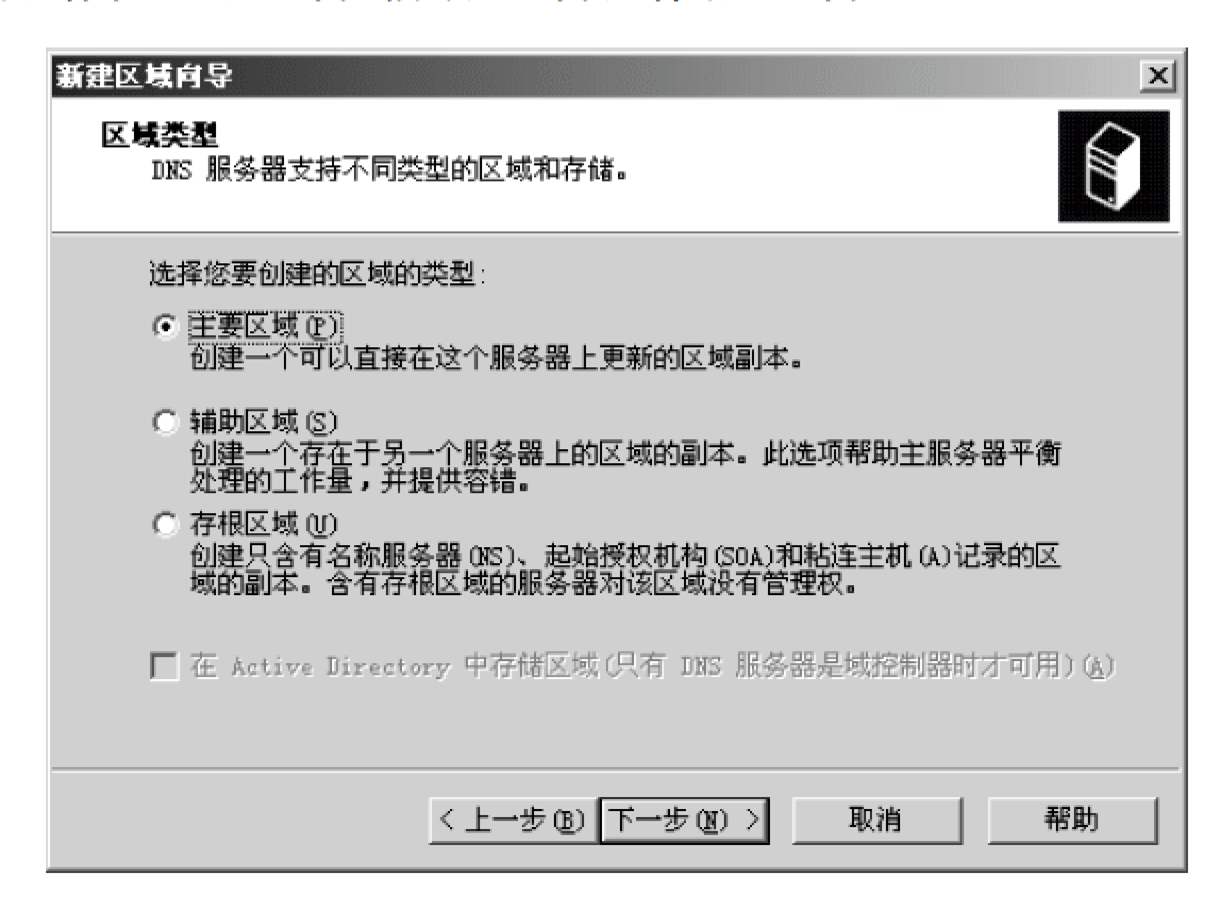


图 2-6　【区域类型】对话框



提示：【主要区域】中的区域记录是自主生成的，是可读可写的。也就是说，该DNS服务器既可以接受新用户的注册，也可以给用户提供名称解析服务。【主要区域】是以文件的形式存放在创建该区域的DNS服务器上。维护【主要区域】的DNS服务器称为该区域的主DNS服务器。

如果一个DNS区域的客户端计算机非常多，为了优化对用户DNS名称解析的服务，可以在另外一台DNS服务器上为该区域创建一个【辅助区域】。【辅助区域】中的区域记录是从【主要区域】复制而来的，是只读的。也就是说，该DNS服务器不能接受新用户的注册请求，只能为已经注册的用户提供名称解析服务。【辅助区域】也是以文件的形式存放在创建该区域的DNS服务器上。维护【辅助区域】的DNS服务器称为该区域的辅助DNS服务器。

【存根区域】是一个区域副本，只包含标识该区域的权威DNS服务器所需的那些资源记录。【存根区域】用来让主持父区域的DNS服务器知道其子区域的权威DNS服务器，从而保持DNS名称解析效率。【存根区域】由以下部分组成：委派区域的起始授权机构(SOA)资源记录、名称服务器(NS)资源记录和主机(A)资源记录。【存根区域】的主服务器是对于子区域具有权威性的一个或多个DNS服务器。

(3) 选择【主要区域】单选按钮，单击【下一步】按钮，打开如图2-7所示的【区域名称】对话框，输入区域名称myexample.com。如果用于Internet上，这里的名称一般是申请的二级域名；对于用于Intranet的内部域名，则可以自行定义，甚至可启用顶级域名。

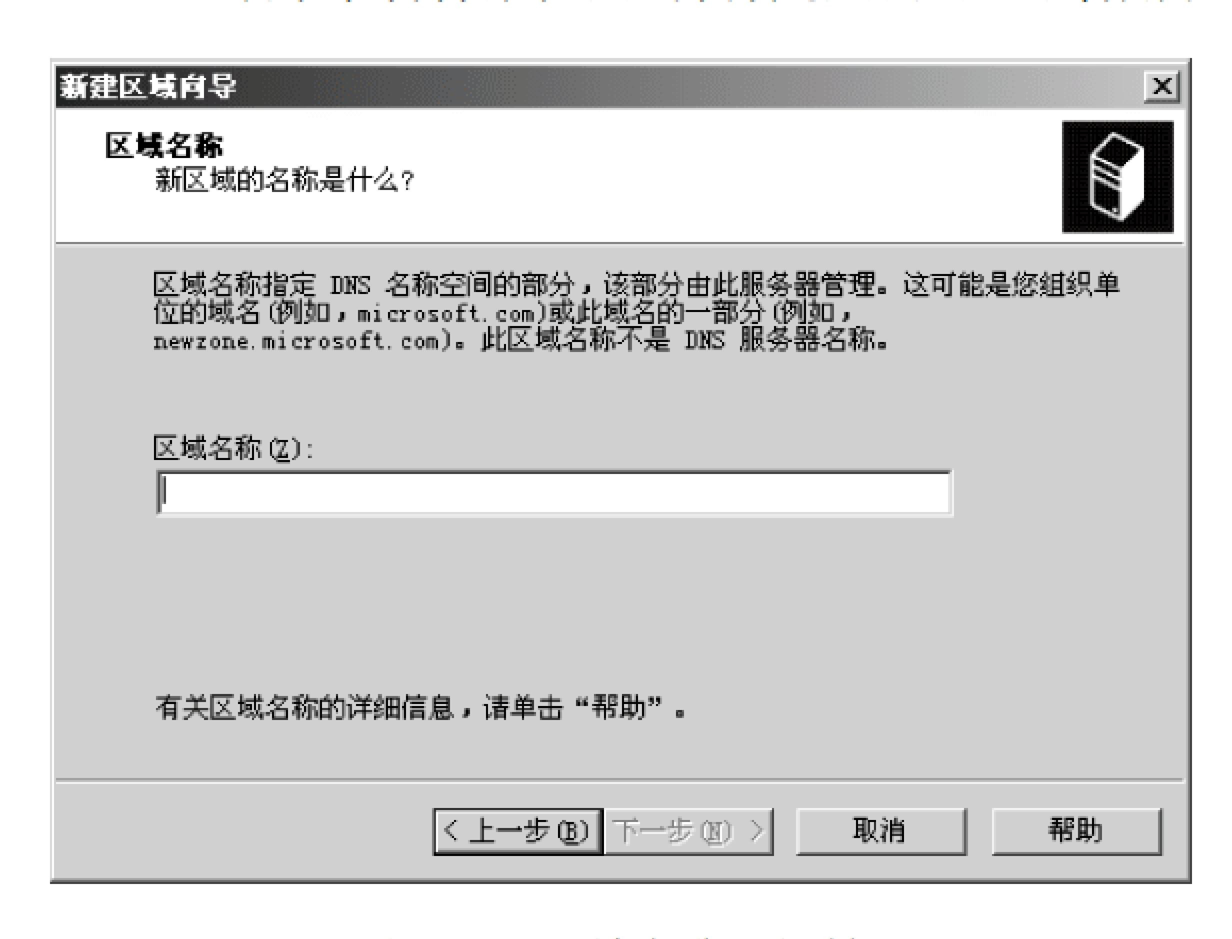


图2-7 【区域名称】对话框

(4) 单击【下一步】按钮，打开如图2-8所示的【区域文件】对话框，定义区域文件。

(5) 单击【下一步】按钮，打开如图2-9所示的【动态更新】对话框，选择【允许非安全和安全动态更新】单选按钮。动态更新的含义是当该区域的客户端计算机的IP地址或主机名发生变化时，这种改变可以动态地在DNS区域记录中进行更改，而无须管理员手工更改。

(6) 单击【下一步】按钮，显示新建区域的基本信息，再单击【完成】按钮。建立区域后，还有一个管理和配置的问题。区域在DNS服务的管理中具有重要地位，它是DNS服务主要的管理单位。用户可通过区域属性来配置DNS服务。



新建区域向导

区域文件
您可以创建一个新区域文件和使用从另一个 DNS 服务器复制的文件。

您想创建一个新的区域文件，还是使用一个从另一个 DNS 服务器复制的现存文件?

创建新文件，文件名为(C):

myexample.com.dns

使用此现存文件(U):

要使用此现存文件，请确认它已经被复制到该服务器上的 %SystemRoot%\system32\dns 文件夹，然后单击“下一步”。

< 上一步(B)　下一步(N) >　取消　帮助

图 2-8　【区域文件】对话框

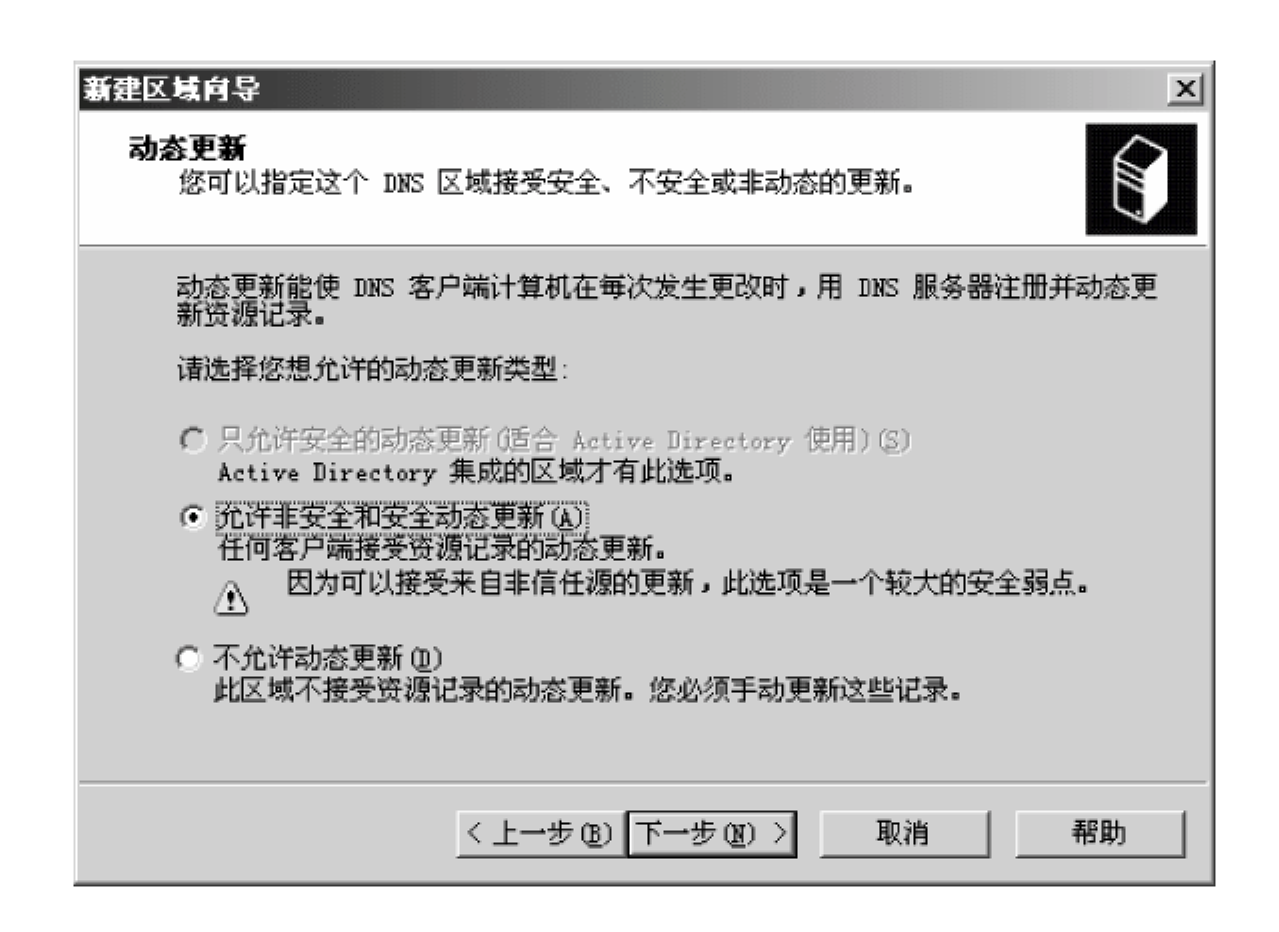


图 2-9　【动态更新】对话框

2.4.2　设置区域属性

在 DNS 控制台树中右击要配置的区域，从弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择如图 2-10 所示的【常规】选项卡，可以进行常规属性设置。其中【状态】表示区域的运行状态，单击右侧的【开始】或【暂停】按钮可以启动或暂停区域，以中断或恢复对该区域的服务。如果要将【类型】的选项改为【辅助区域】，就需要指定另一个 DNS 服务器的 IP 地址作为获得此区域的更新信息的源。可在【区域文件名】文本框中更改文件名称。

管理员还可设置动态更新功能。动态更新允许 DNS 客户机变动时，使用 DNS 服务器注册和动态地更新其资源记录，这样就不必手工管理区域记录了。这对于频繁移动或改变位置并使用 DHCP 的客户机特别有用。在【允许动态更新】列表中选择【非安全】或【无】来启用或禁用区域的动态更新功能。

DNS 服务器加载区域时，使用起始授权机构(SOA)和名称服务器(NS)两种资源记录来确定区域的授权属性，它们在区域配置中具有特殊作用。在默认情况下，添加新区域向导



会自动创建这些记录。

起始授权机构(SOA)资源记录在任何标准区域中都是第一个记录，指明区域的源名称，包含作为区域信息主要来源的服务器的名称，还表示该区域的其他基本属性。在区域属性设置对话框中选择如图 2-11 所示的【起始授权机构】选项卡，可以设置以下各项属性。

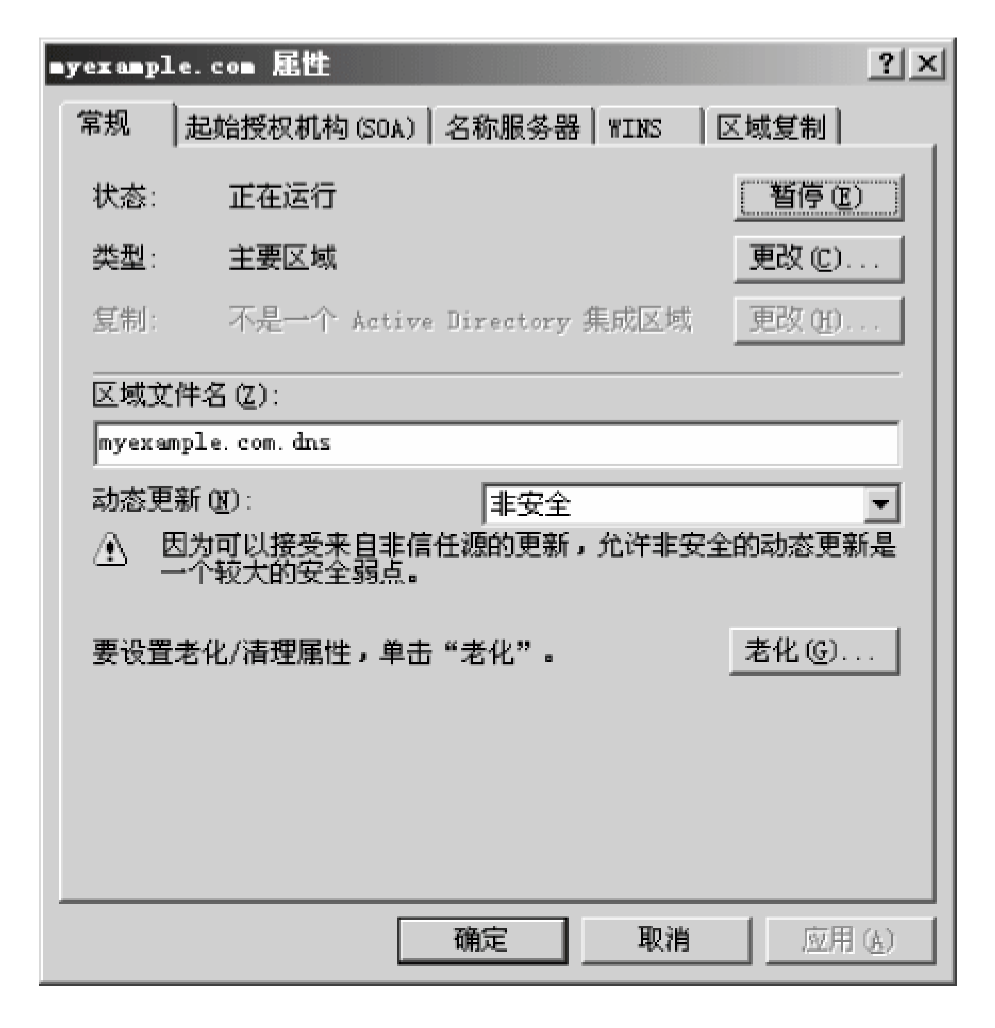



图 2-10 【常规】选项卡



图 2-11 【起始授权机构】选项卡

- 序列号：表示该区域文件的修订版本号。每次区域中的资源记录改变时，该值便会增加。该值很重要，它使改动过的区域都可在后续传送中复制到其他辅助服务器上。
- 主服务器：区域的主 DNS 服务器的主机名。
- 负责人：管理区域的负责人的电子邮件地址。注意在该电子邮件名称中使用英文句点“.”代替符号“@”。
- 刷新间隔：以秒计算的时间，表示辅助 DNS 服务器更新的频率。当刷新间隔到期时，辅助 DNS 服务器将其本地 SOA 记录的序列号同主 DNS 服务器的当前 SOA 记录的序列号比较，如果二者不同，则辅助 DNS 服务器从主 DNS 服务器请求区域传送。
- 重试间隔：以秒计算的时间，是辅助服务器在重试失败的区域传送之前等待的时间。
- 过期时间：以秒计算的时间，是指在该区域数据没有从其源服务器刷新的最长期限，超过该期限，辅助 DNS 服务器将停止响应查询。默认情况下，该时间段为 1 天(24 小时)。
- 最小(默认)TTL：适用于区域内带有未指定记录特定 TTL 的所有资源记录的最小生存时间(TTL)值。
- 此记录的 TTL：表示该数据在客户端存留的时间。

名称服务器(NS)资源记录用于标记被指定为区域权威服务器的 DNS 服务器，这些服务器能给出权威性应答。在区域属性设置对话框中选择如图 2-12 所示的【名称服务器】选项卡，即可编辑名称服务器列表，可根据需要将其他 DNS 服务器指定为区域的权威服务器。



2.4.3　设置区域复制

主 DNS 服务器可以将区域复制到其他 DNS 服务器，以提高容错性能和服务器性能。在区域属性设置对话框中选择如图 2-13 所示的【区域复制】选项卡，可以设置有关选项。

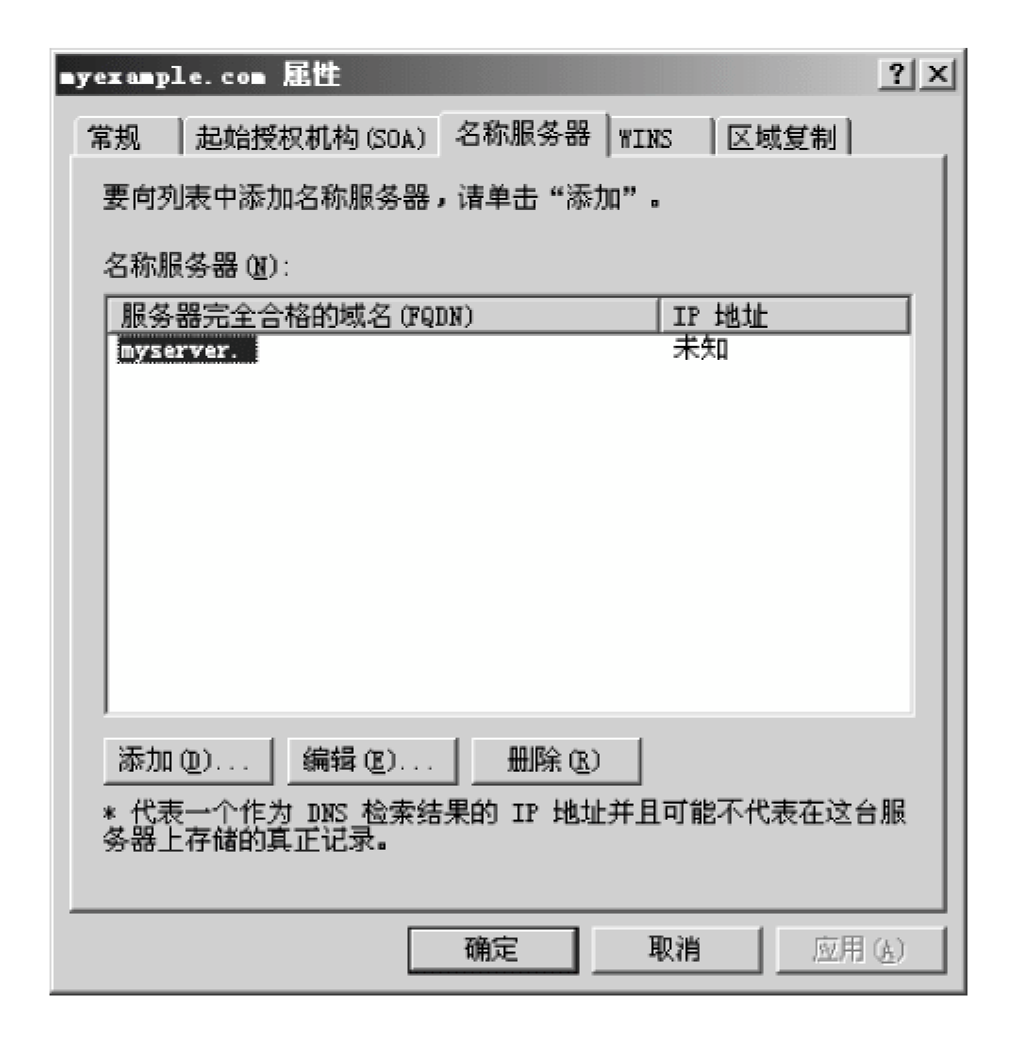


图 2-12　【名称服务器】选项卡

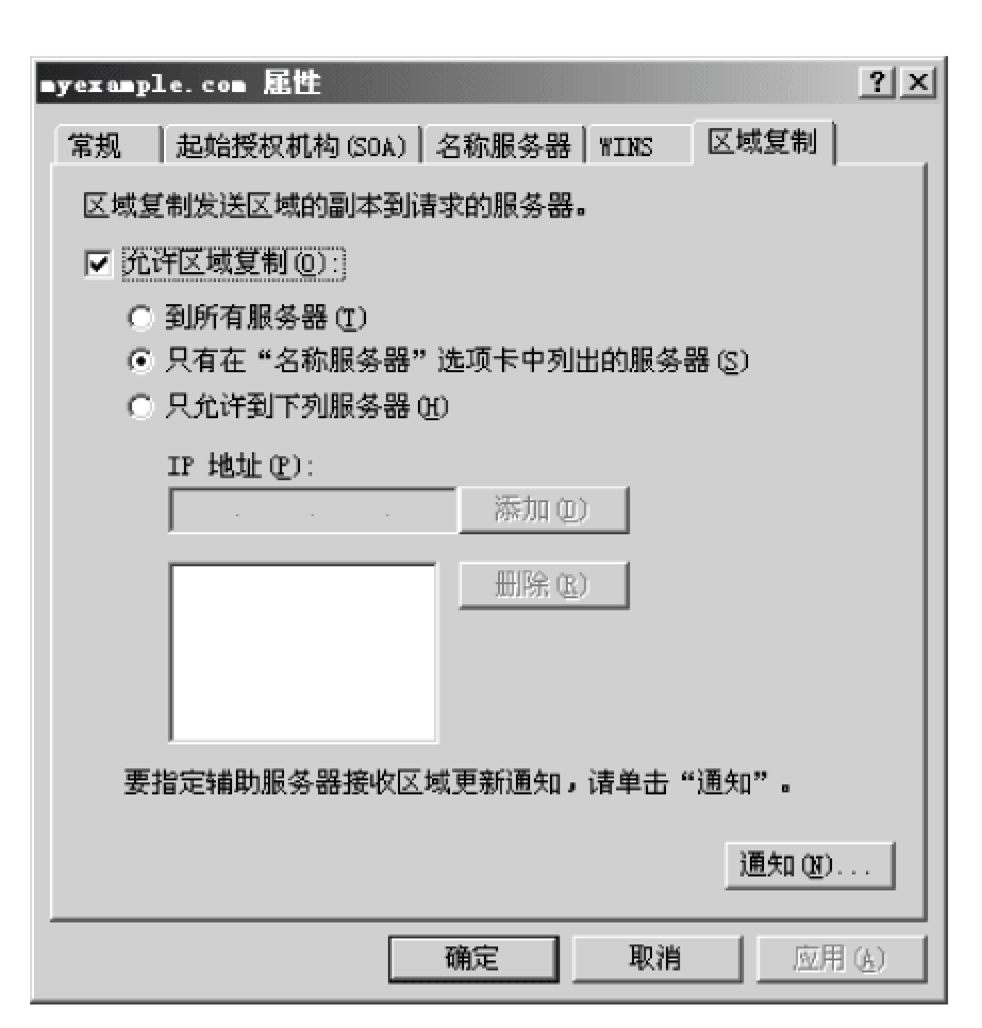


图 2-13　【区域复制】选项卡

2.5　建立和管理 DNS 域

建立完区域以后，可以进一步增加域名的层次，在区域的下面建立 DNS 域(在域中可再建子域)，在域中再建立资源记录。例如，在 www.myexample.com 区域中，再建立 ee 和 cs 等域。建立域的步骤如下：

在 DNS 控制台的目录树中选择一个区域，右击此区域，从弹出的快捷菜单中选择【新建域】命令，打开如图 2-14 所示的【新建 DNS 域】对话框。在文本框中输入新建的域，如 ee，单击【确定】按钮，这样就建立了一个绝对域名为 ee.myexample.com 的域，它是区域 myexample.com 中的域。



图 2-14　【新建 DNS 域】对话框

2.6　建立和管理 DNS 资源记录

拥有了自己的域名以后，下一步就是要进行相应的管理。域名的管理其实就是对相关记录进行增加、删除和修改之类的操作。相关记录包括四种，分别是主机记录、别名记录、邮件交换器记录和其他资源记录。四种不同记录相辅相成，各司其职，又互相补充。通过对它们进行不同的操作来完成域名管理。



2.6.1 主机记录

主机资源记录(A记录)是用来指定域名对应的IP地址的记录。主机记录就是把计算机的域名和IP地址绑定,告诉DNS服务器,当有域名查询请求的时候,将把它引导向主机记录所指定的IP地址。例如,有一条主机记录www.microsoft.com-> 200.100.100.100,访问www.microsoft.com的请求就会通过DNS服务器解析到200.100.100.100。

新建主机记录的操作步骤如下:

(1) 在DNS控制台的目录树中选择一个区域,右击此区域,从弹出的快捷菜单中选择【新建主机】命令,打开如图2-15所示的【新建主机】对话框。

(2) 在【名称】文本框中输入新建的主机名,如www;在【IP地址】文本框中输入新建的主机名对应的IP地址。

(3) 如果还同时想建立与此主机记录有关的指针记录,可以选择【创建相关的指针(PTR)记录】复选框,这样,反向搜索区域中将自动添加一个对应的记录。

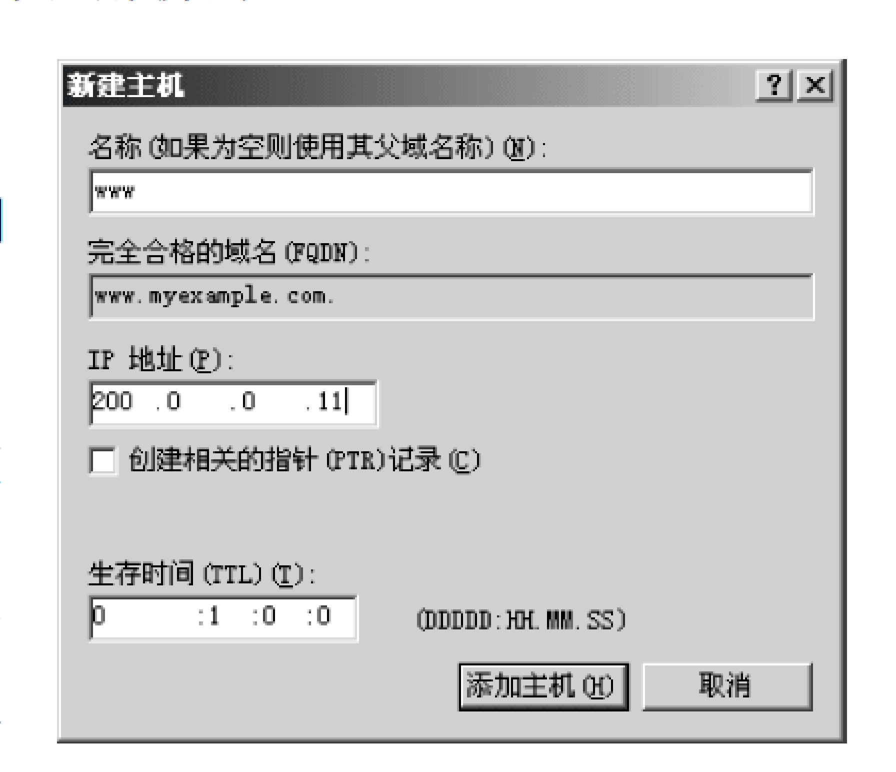


图 2-15 【新建主机】对话框

(4) 单击【添加主机】按钮,这样就建立了一个绝对域名为www.myexample.com的主机名,它是区域myexample.com中的主机。

2.6.2 别名记录

别名资源记录(CNAME记录)允许将多个名字映射到同一台计算机。通常用于同时提供WWW和MAIL服务的计算机。例如,有一台计算机域名为host.myexample.com,它同时提供WWW和MAIL服务。为了便于用户访问服务,可以为该计算机设置两个别名记录:WWW和MAIL。这两个别名的全称就是www.myexample.com和mail.myexample.com。实际上它们都指向host.myexample.com。同样的方法可以用于多个域名需要指向同一服务器IP,此时就可以将一个域名做A记录指向服务器IP,然后将其他的域名做CNAME记录到之前做A记录的域名上。这样当服务器IP地址变更时就可以不必麻烦地一个一个域名更改指向了,只需要更改做A记录的那个域名,其他做别名的那些域名的指向也将自动更改到新的IP地址上。新建别名记录的操作步骤如下:

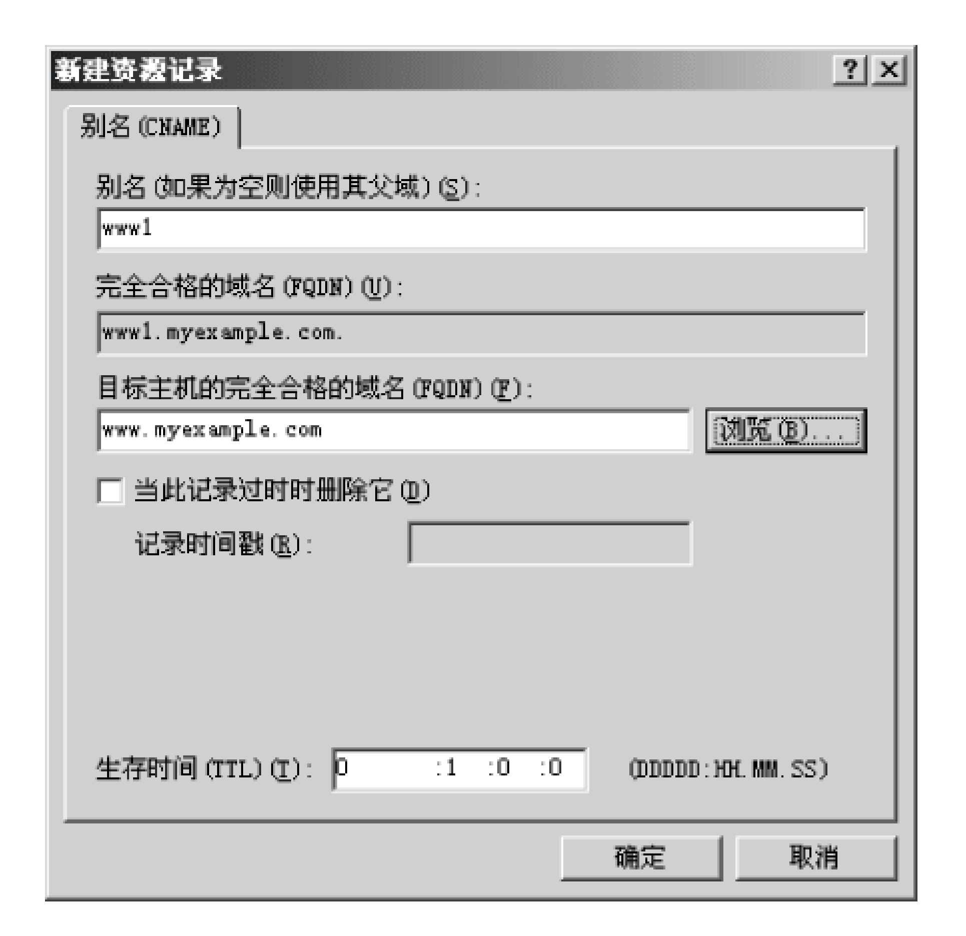


图 2-16 【新建别名】对话框

在DNS控制台的目录树中选择一个区域,右击此区域,从弹出的快捷菜单中选择【新建别名】命令,打开如图2-16所示的【新建别名】对



话框。在【别名】文本框中输入新建的别名，这里是相对父域的名称，如 www1 表示 www1. myexample. com；在【目标主机的完全合格的域名】文本框中输入该别名对应的主机的完整域名，如 www. myexample. com，单击【确定】按钮。

2.6.3　邮件交换器记录

邮件交换器记录（MX 记录）指向一个邮件服务器，用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。例如，当 Internet 上的某用户要发一封信给 user@mail. myexample. com 时，该用户的邮件系统通过 DNS 查找 mail. myexample. com 这个域名的 MX 记录，如果 MX 记录存在，用户计算机就将邮件发送到 MX 记录所指定的邮件服务器上。新建邮件交换器记录的操作步骤如下：

（1）在 DNS 控制台的目录树中选择一个区域，右击此区域，从弹出的快捷菜单中选择【新建邮件交换器】命令，打开如图 2-17 所示的【新建邮件交换器】对话框。

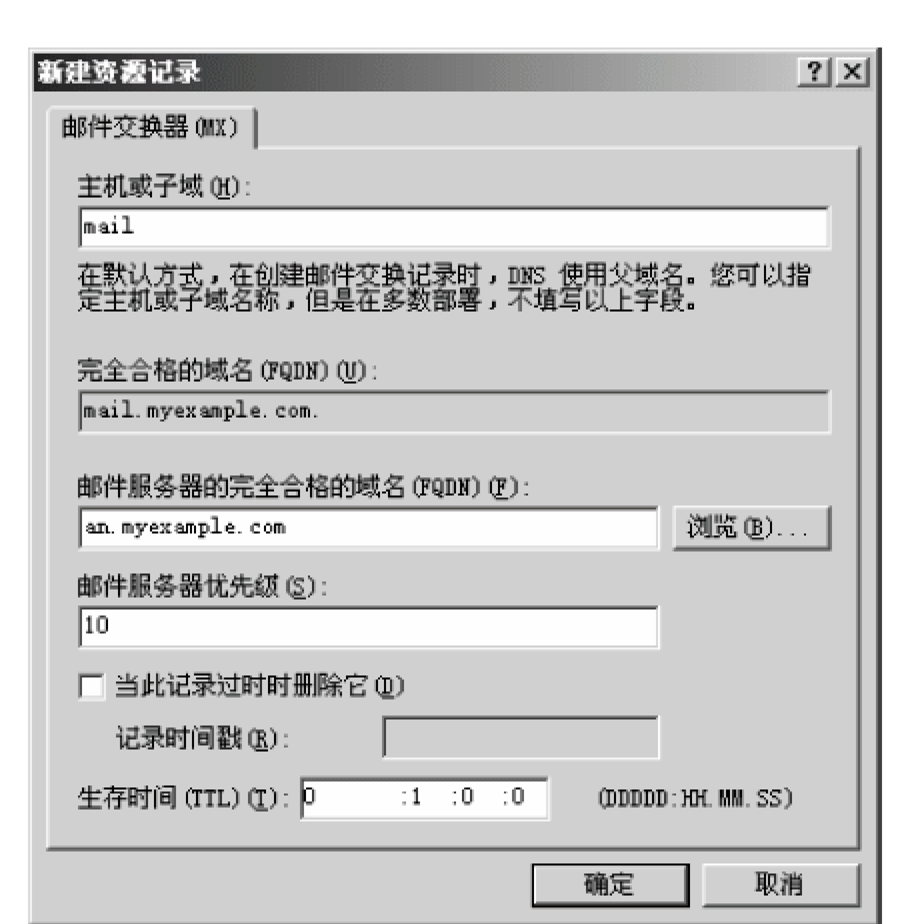


图 2-17　【新建邮件交换器】对话框

（2）在【主机或子域】文本框中输入此邮件交换器记录负责的域名，这里是相对父域的名称。如输入名称为 mail，父域为 myexample. com，则此邮件交换器所负责的域名为 mail. myexample. com。

（3）在【邮件服务器的完全合格的域名】文本框中输入负责处理上述域（由【主机或子域】文本框指定）邮件的邮件服务器的全称域名，如 an. myexample. com。发送或交换到邮件交换器记录所负责域中的邮件将由该邮件服务器处理。

（4）在【邮件服务器优先级】文本框中输入一个 0～65535 的数值，当一个区域中有多个邮件交换器记录时，这个数值决定邮件服务的优先级，邮件优先发给值小的邮件服务器。

（5）单击【确定】按钮，添加邮件交换器记录成功。这样所有发送给“用户名@mail. myexample. com”的邮件都会被 DNS 系统进行 MX 记录解析，根据解析结果将把邮件转发到 an. myexample. com 这台邮件服务器上。

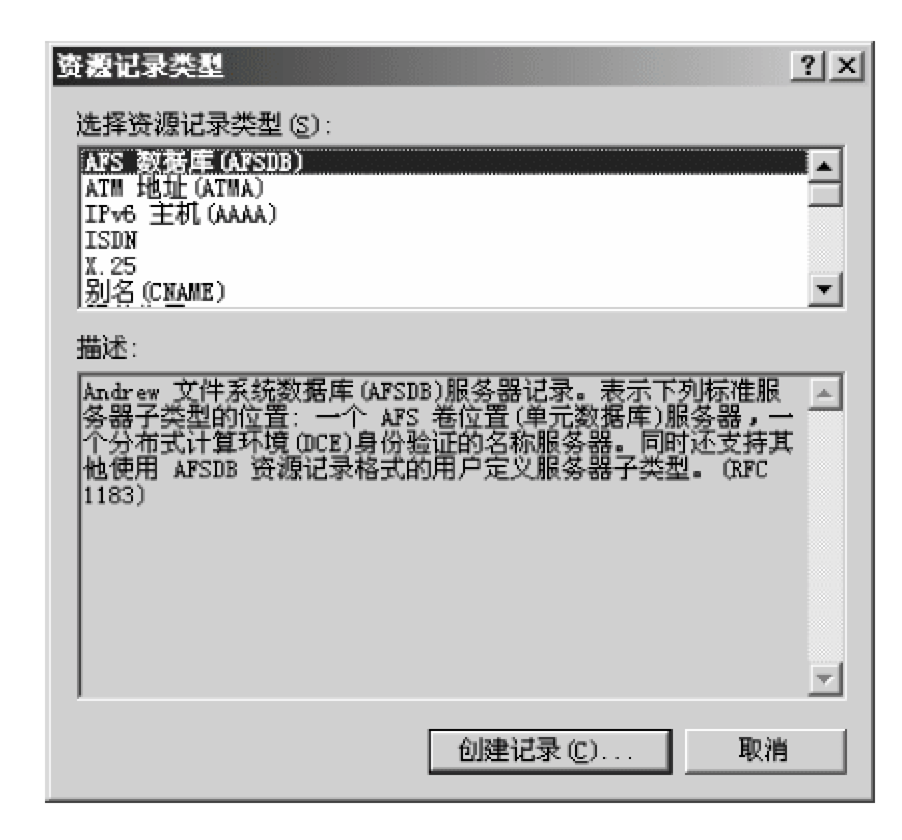


图 2-18　【资源记录类型】对话框

2.6.4　其他资源记录

还可以在 DNS 服务器上建立其他资源记录，用户可以根据需要在 DNS 控制台中添加。添加步骤如下：

在 DNS 控制台的目录树中选择一个区域，右击此区域，从弹出的快捷菜单中选择【其他新记录】命令，打开如图 2-18 所示的【资源记录类型】对话框。在【选择资源记录类型】列表框中选择要新建



的资源记录类型，然后单击【创建记录】按钮，即可打开相应的对话框进行设置。

2.7　DNS 客户端的设置

尽管 DNS 服务器已经创建成功，并且创建了合适的域名，可是在客户机的浏览器中却无法使用域名访问网站。这是因为虽然已经有了 DNS 服务器，但客户机并不知道 DNS 服务器在哪里，因此不能识别用户输入的域名。用户必须在客户端手动设置 DNS 服务器的 IP 地址才行。设置步骤如下：

(1) 依次选择【开始】→【设置】→【网络连接】→【本地连接】命令，打开【本地连接状态】对话框。

(2) 在【常规】选项卡的【此连接使用下列项目】列表框中，双击【Internet 协议(TCP/IP)】，打开如图 2-19 所示的【Internet 协议(TCP/IP)属性】对话框。

(3) 在【常规】选项卡中，选择【使用下面的 DNS 服务器地址】单选按钮。在【首选 DNS 服务器】文本框中，输入首选 DNS 服务器的 IP 地址，如 200.0.0.100；如果有备用 DNS 服务器，在【备用 DNS 服务器】文本框中，输入备用 DNS 服务器的 IP 地址，如 200.0.0.200，单击【确定】按钮，即可使用服务器提供的 DNS 服务。

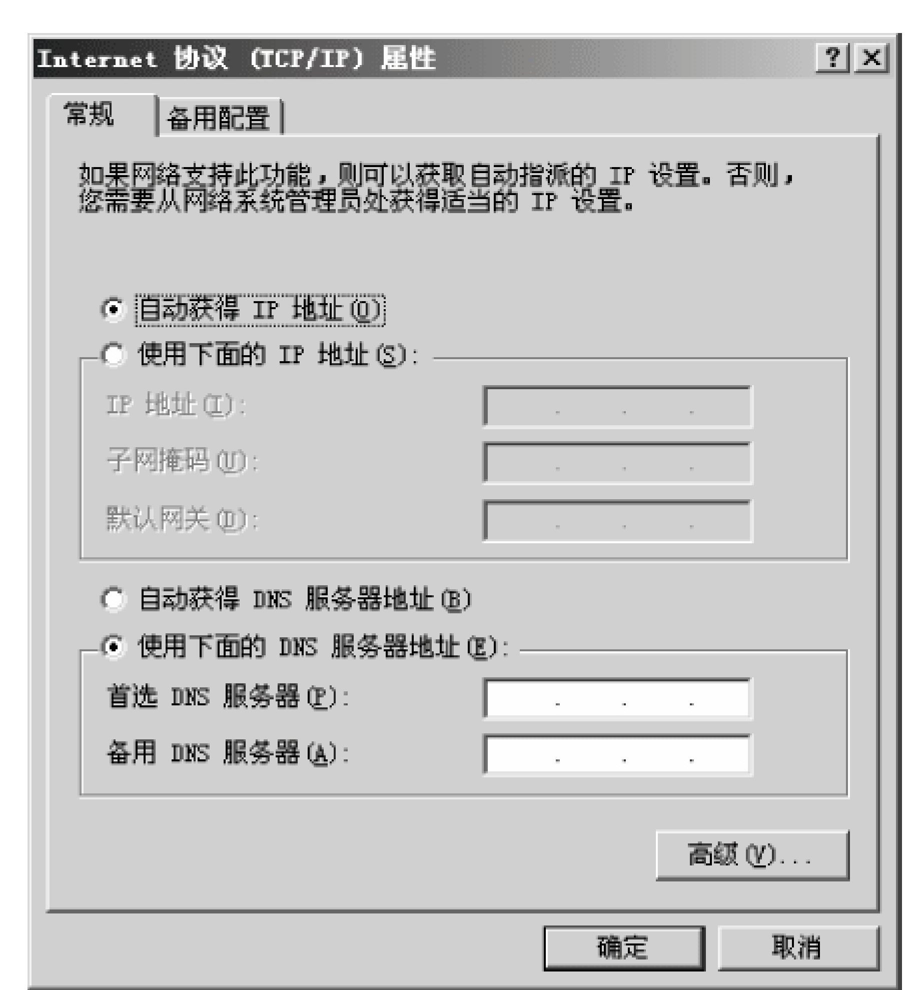


图 2-19　【Internet 协议(TCP/IP)属性】对话框

2.8　疑难解答

(1) 安装 DNS 服务器后，如果 DNS 控制台的目录树中，没有想要管理的 DNS 服务器应该如何添加一台 DNS 服务器？

在 DNS 控制台的目录树中，右击 DNS 根节点，从弹出的快捷菜单中选择【连接到 DNS 服务器】命令，在打开的【连接到 DNS 服务器】对话框中选择【这台计算机】单选按钮，把本地的这台计算机作为 DNS 服务器进行管理，或者选择【下列计算机】单选按钮，在下面的文本框中输入需要管理的某台 DNS 服务器的名字或 IP 地址来对其进行管理。

(2) 当 DNS 客户机变动时，为了使用 DNS 服务器注册和动态地更新其资源记录，应该如何设置？

在 DNS 控制台树中右击要配置的区域，从弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择如图 2-10 所示的【常规】选项卡，在【动态更新】下拉列表框中选择【非安全】选项来启用区域的动态更新功能。

(3) 如何知道 DNS 服务器是否能够成功地对某域名进行解析？

可以在向此 DNS 服务器发出解析请求的客户机上运行“ping 域名”来进行测试。如果



ping 通，证明 DNS 服务器能够成功地对此域名进行解析。如果没有 ping 通，则说明 DNS 服务器没有解析成功。

习　　题

1. 填空题

（1）DNS 域名称空间是一种________状结构。

（2）DNS 服务用于将________地址解析为与此对应的________地址。

2. 选择题

（1）（　　）记录指向一个邮件服务器，用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。

A. A　　B. CNAME　　C. MX　　D. SOA

（2）（　　）表示该区域文件的修订版本号。每次区域中的资源记录改变时，该值便会增加。该值很重要，它使改动过的区域都可在后续传送中复制到其他辅助服务器上。

A. TTL　　B. 序列号　　C. 过期时间　　D. 重试间隔

3. 思考题

（1）DNS 区域有哪几种类型？

（2）DNS 资源记录有哪些种类？



第3章　DHCP服务器配置与管理

本章要点

- DHCP 服务的工作原理
- 创建和设置 DHCP 作用域

在使用 TCP/IP 协议的网络上，每一台计算机都拥有唯一的计算机名和 IP 地址。IP 地址可以鉴别它所连接的主机和子网，当用户将计算机从一个子网移动到另一个子网的时候，一定要改变该计算机的 IP 地址。如采用静态 IP 地址的分配方法将增加网络管理员的负担，而 DHCP 可以让管理员将 IP 地址动态地分配给局域网中的计算机，从而减轻了网络管理员的负担。

3.1　了解 DHCP 服务

动态主机配置协议，简称 DHCP(Dynamic Host Configuration Protocol)，是 TCP/IP 协议族中的一种，主要是用来给网络客户机分配动态的 IP 地址。这些被分配的 IP 地址都是 DHCP 服务器预先保留的一个由多个地址组成的 IP 地址数据库。

3.1.1　DHCP 服务概述

使用 DHCP 时必须在网络上有一台 DHCP 服务器，而局域网内的其他计算机作为 DHCP 客户端，如图 3-1 所示。当 DHCP 客户端程序发出一个信息，要求获取一个动态的 IP 地址时，DHCP 服务器会根据目前已经配置的地址，提供一个可供使用的 IP 地址和子网掩码给客户端，这个过程是自动完成的。

在网络中配置 DHCP 服务器有如下优点：

(1) 管理员可以集中为整个互联网指定通用和特定子网的 TCP/IP 参数，并且可以定义使用保留地址的客户机的参数。

(2) 提供安全可信的配置。DHCP 避免了在每台计算机上手工输入数值引起的配置错误，还能防止网络上计算机配置地址的冲突。

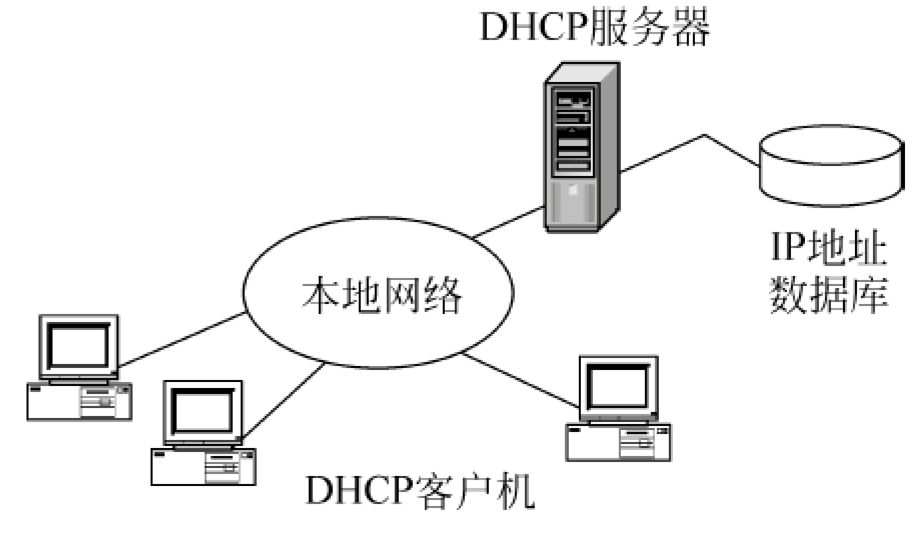


图 3-1　使用 DHCP 服务的网络

(3) 使用 DHCP 服务器能大大减少配置花费的开销和重新配置网络上计算机的时间，服务器可以在指派地址租约时配置所有的附加配置值。

(4) 客户机不需手工配置 TCP/IP。

(5) 客户机在子网间移动时，旧的 IP 地址自动释放以便再次使用。在再次启动客户机时，DHCP 服务器会自动为客户机重新配置 TCP/IP。

(6) 大部分路由器可以转发 DHCP 配置请求，因此，互联网的每个子网并不都需要 DHCP 服务器。

3.1.2　DHCP 服务的工作原理

DHCP 允许有如下三种类型的地址分配：

- DHCP 允许手工配置，管理员可为特定的某个计算机配置特定的地址。
- 管理员可为第一次连接到网络的计算机分配一个固定的地址，该计算机以后就使用该地址。
- DHCP 允许完全动态配置，服务器可使计算机在一段时间内租用一个地址，租用时间到期时释放地址。

DHCP 分配 IP 地址的过程如图 3-2 所示。

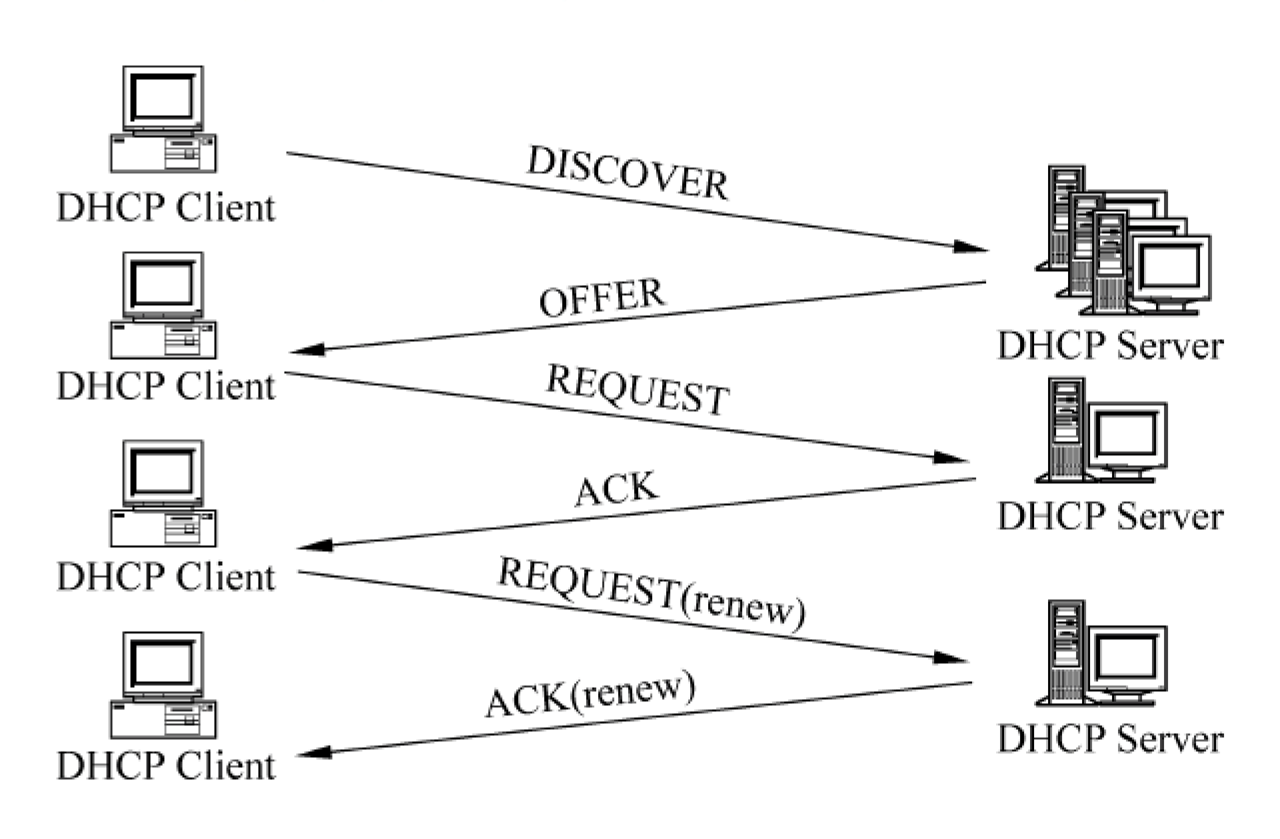


图 3-2　DHCP 分配 IP 地址的过程

(1) 发现阶段，即 DHCP 客户机寻找 DHCP 服务器的阶段。DHCP 客户机以广播方式(因为 DHCP 服务器的 IP 地址对于客户机来说是未知的)发送 DHCPDISCOVER 发现信息来寻找 DHCP 服务器，即向地址 255.255.255.255 发送特定的广播信息。网络上每一台安装了 TCP/IP 协议的主机都会接收到这种广播信息，但只有 DHCP 服务器才会做出响应。

(2) 提供阶段，即 DHCP 服务器提供 IP 地址的阶段。在网络中接收到 DHCPDISCOVER 发现信息的 DHCP 服务器都会做出响应，它从尚未出租的 IP 地址中挑选一个分配给 DHCP 客户机，向 DHCP 客户机发送一个包含出租的 IP 地址和其他设置的 DHCPOFFER 提供信息。

(3) 选择阶段，即 DHCP 客户机选择某台 DHCP 服务器提供的 IP 地址的阶段。如果有多



台 DHCP 服务器向 DHCP 客户机发来的 DHCPOFFER 提供信息,则 DHCP 客户机只接受第一个收到的 DHCPOFFER 提供信息,然后它就以广播方式回答一个 DHCPREQUEST 请求信息,该信息中包含向它所选定的 DHCP 服务器请求 IP 地址的内容。之所以要以广播方式回答,是为了通知所有的 DHCP 服务器,它将选择某台 DHCP 服务器所提供的 IP 地址。

(4) 确认阶段,即 DHCP 服务器确认所提供的 IP 地址的阶段。当 DHCP 服务器收到 DHCP 客户机回答的 DHCPREQUEST 请求信息之后,它便向 DHCP 客户机发送一个包含它所提供的 IP 地址和其他设置的 DHCPACK 确认信息,告诉 DHCP 客户机可以使用它所提供的 IP 地址。然后 DHCP 客户机便将其 TCP/IP 协议与网卡绑定,另外,除 DHCP 客户机选中的服务器外,其他的 DHCP 服务器都将收回曾提供的 IP 地址。

(5) 重新登录。以后 DHCP 客户机每次重新登录网络时,就不需要再发送 DHCPDISCOVER 发现信息了,而是直接发送包含前一次所分配的 IP 地址的 DHCPREQUEST 请求信息。当 DHCP 服务器收到这一信息后,它会尝试让 DHCP 客户机继续使用原来的 IP 地址,并回答一个 DHCPACK 确认信息。如果此 IP 地址已无法再分配给原来的 DHCP 客户机使用(比如此 IP 地址已分配给其他 DHCP 客户机使用),则 DHCP 服务器给 DHCP 客户机回答一个 DHCPNACK 否认信息。当原来的 DHCP 客户机收到此 DHCPNACK 否认信息后,它就必须重新发送 DHCPDISCOVER 发现信息来请求新的 IP 地址。

(6) 更新租约。DHCP 服务器向 DHCP 客户机出租的 IP 地址一般都有一个租借期限,期满后 DHCP 服务器便会收回出租的 IP 地址。如果 DHCP 客户机要延长其 IP 租约,则必须更新其 IP 租约。DHCP 客户机启动时和 IP 租约期限过一半时,DHCP 客户机都会自动向 DHCP 服务器发送更新其 IP 租约的信息。

3.2 DHCP 服务器的安装

要使用 DHCP 服务,就要安装 DHCP 服务器。下面以 Windows Server 2003 为例来介绍。首先检查本地计算机是否已安装 DHCP 服务组件:依次选择【开始】→【程序】→【管理工具】命令,此时如没有出现 DHCP 子菜单,则需按以下步骤安装:

(1) 依次选择【开始】→【设置】→【控制面板】命令,打开【控制面板】窗口。

(2) 在【控制面板】窗口中,双击【添加或删除程序】快捷方式,打开【添加或删除程序】对话框。

(3) 在【添加或删除程序】对话框中,单击左边的【添加/删除 Windows 组件】按钮,打开如图 3-3 所示的【Windows 组件向导】对话框。

(4) 在其中的【组件】列表中,双击【网络服务】复选框,打开如图 3-4 所示的【网络服务】对话框。在其中选中【动态主机配置协议(DHCP)】复选框,单击【确定】按钮。

(5) 在【Windows 组件向导】对话框中,单击【下一步】按钮,出现安装提示。在光驱中插入 Windows Server 2003 系统安装盘后,完成安装。

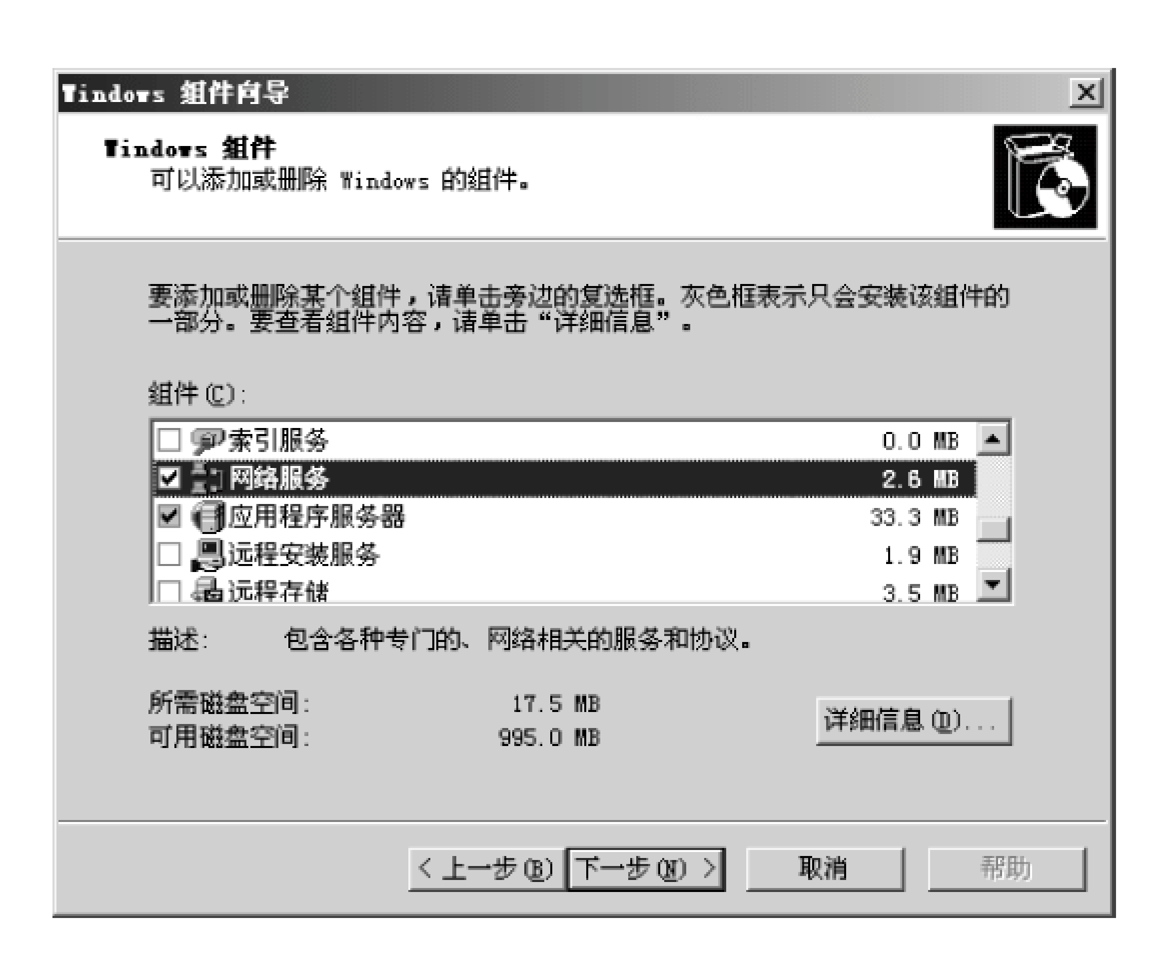




图 3-3　【Windows 组件向导】对话框

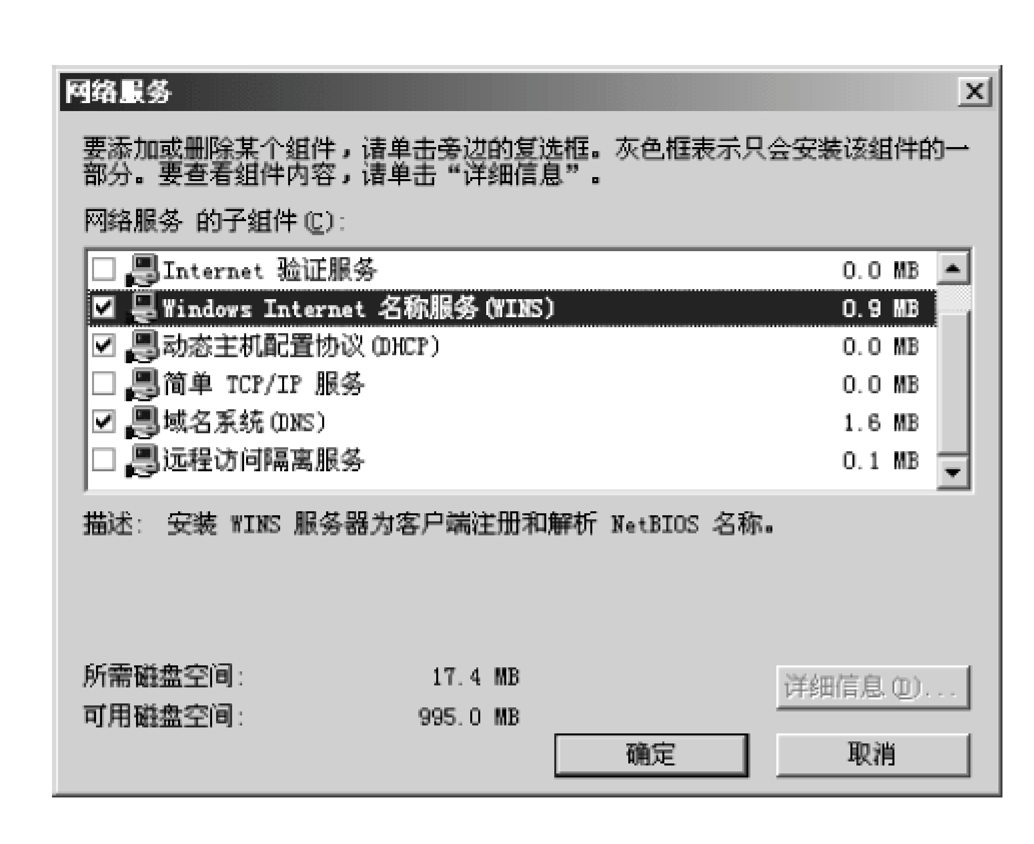


图 3-4　【网络服务】对话框

3.3　DHCP 服务器级的管理

3.3.1　DHCP 控制台

DHCP 服务安装完成以后，会自动在【管理工具】菜单中增加一个 DHCP 子菜单。依次选择【开始】→【程序】→【管理工具】→DHCP 命令，打开如图 3-5 所示的 DHCP 控制台窗口，即可对 DHCP 服务进行配置管理。

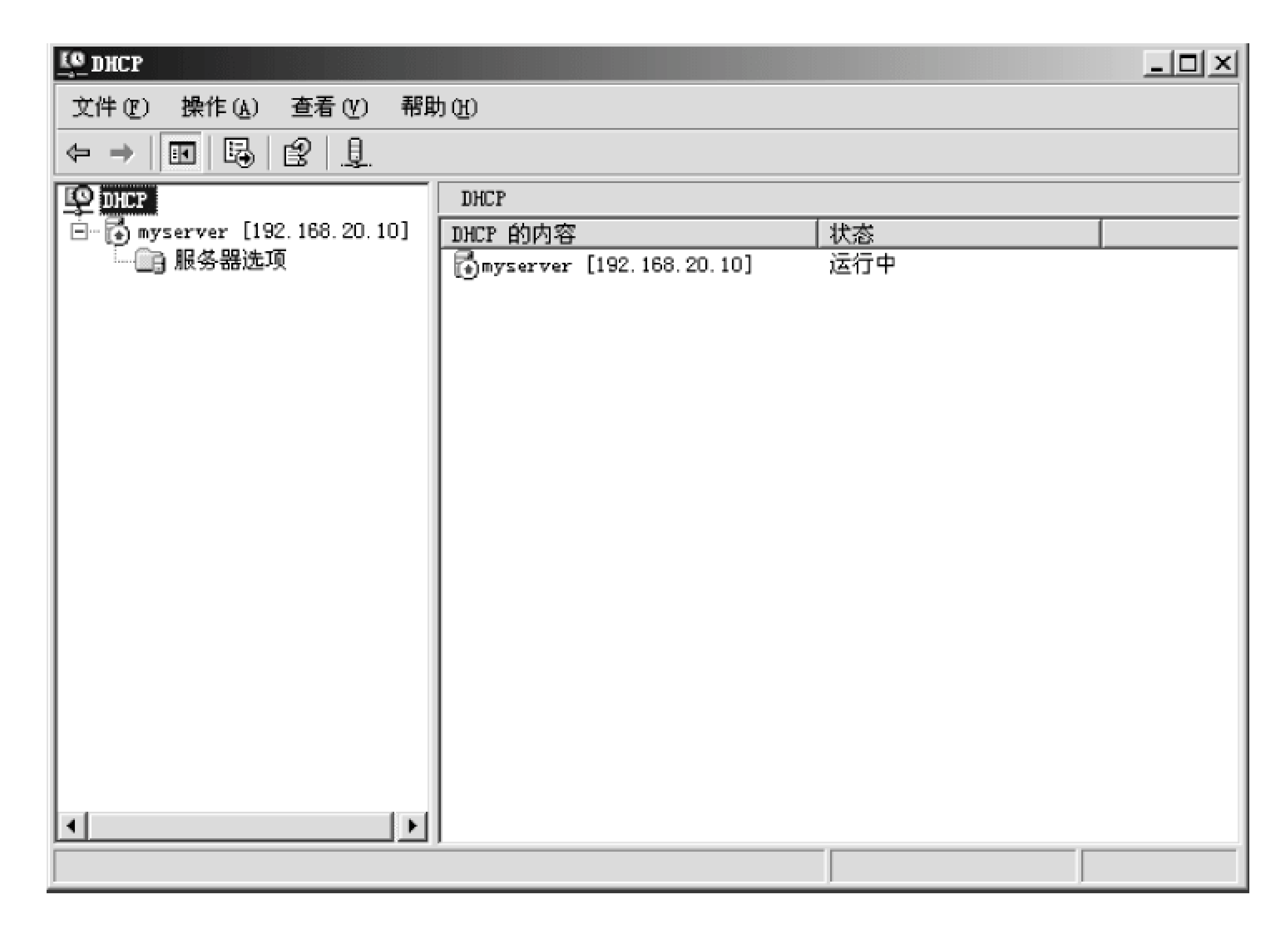


图 3-5　DHCP 控制台窗口

安装 DHCP 服务器后，系统自动将本机默认的 DHCP 服务器添加到 DHCP 控制台的目录树中。当然，还可将网上的其他 Windows 2003 DHCP 服务器添加到控制台中进行管



理。DHCP 服务器的管理层次为：DHCP→DHCP 服务器→超级作用域→作用域→IP 地址范围。

3.3.2 DHCP 服务器级的基本设置

在 DHCP 控制台中，可以进行 DHCP 服务器级的基本设置。在控制台目录树中，选择相应的 DHCP 服务器，右击，从弹出的快捷菜单中选择【所有任务】命令，再从相应的下拉菜单中选择【开始】、【停止】、【暂停】或【重新启动】等命令，即可对整个 DHCP 服务器进行相应的管理。

还可以在 DHCP 控制台中设置 DHCP 服务器的冲突检测。为确认网络上没有其他主机使用 DHCP 服务器提供的 IP 地址，从而避免 IP 地址冲突，需要配置 DHCP 服务器执行冲突检测，以确认分配给 DHCP 客户端的 IP 地址没有被其他主机使用。

配置方式如下：在 DHCP 控制台中，右击 DHCP 服务器名，从弹出的快捷菜单中选择【属性】命令，打开如图 3-6 所示的【属性】对话框。然后单击【高级】标签，打开【高级】选项卡，在【冲突检测次数】栏输入需要 DHCP 服务器进行冲突检测的次数，默认为 0，即不进行冲突检测。DHCP 服务器的冲突检测是在发出 DHCPOFFER 广播数据包之前，因此过多的检测次数会增加 DHCP 服务器应答 DHCP 客户端租约请求的时延。建议设置不超过三次的冲突检测次数。

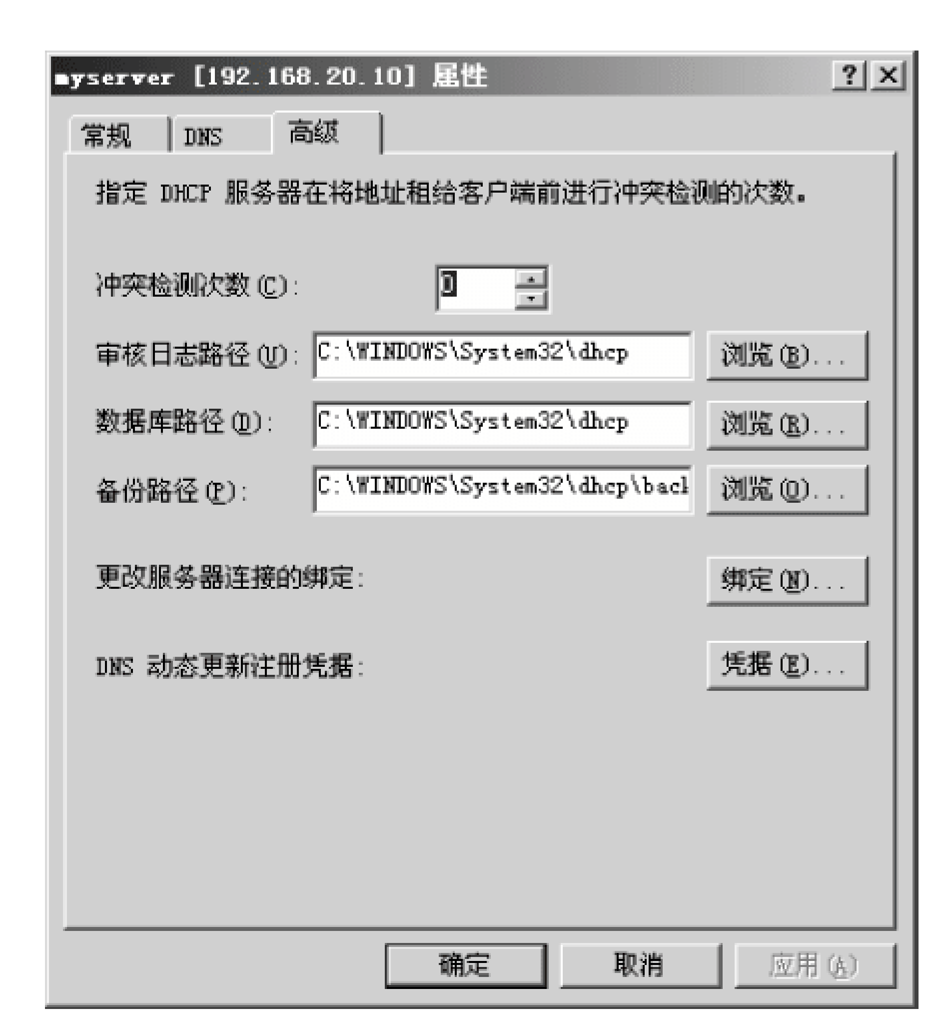


图 3-6 【属性】对话框

3.4 创建和设置 DHCP 作用域

DHCP 作用域是本地逻辑子网中可以使用的 IP 地址的集合，如 192.168.0.1～192.168.0.254。DHCP 服务器只能使用作用域中定义的 IP 地址来分配给 DHCP 客户端，因此，必须创建作用域才能让 DHCP 服务器分配 IP 地址给 DHCP 客户端。DHCP 作用域定义的 IP 地址范围是连续的，并且每个子网只能有一个作用域。如果想要使用单个子网内的不连续的 IP 地址范围，则必须先定义作用域，然后设置所需的排除范围。DHCP 作用域中为 DHCP 客户端分配的 IP 地址必须没有被其他主机所占用，否则必须对 DHCP 作用域设置排除选项，将已被其他主机使用的 IP 地址排除在此 DHCP 作用域之外。

每一个作用域具有以下属性：

- 可以租用给 DHCP 客户端的 IP 地址范围，可在其中设置排除选项，设置为排除的 IP 地址将不分配给 DHCP 客户端使用。



- 子网掩码，用于确定给定 IP 地址的子网，此选项创建作用域后无法修改。
- 创建作用域时指定的名称。
- 租约期限值。
- DHCP 作用域选项，如 DNS 服务器、路由器 IP 地址和 WINS 服务器地址等。
- 保留（可选），用于确保某个确定 MAC 地址的 DHCP 客户端总是能从此 DHCP 服务器获得相同的 IP 地址。

3.4.1　创建 DHCP 作用域

创建 DHCP 作用域的过程如下所示：

（1）在 DHCP 控制台中，右击服务器 myserver，从弹出的快捷菜单中选择【新建作用域】命令，进入【新建作用域】向导。

（2）单击【下一步】按钮，打开如图 3-7 所示的【作用域名】对话框。在其中给出作用域名称为 jz。

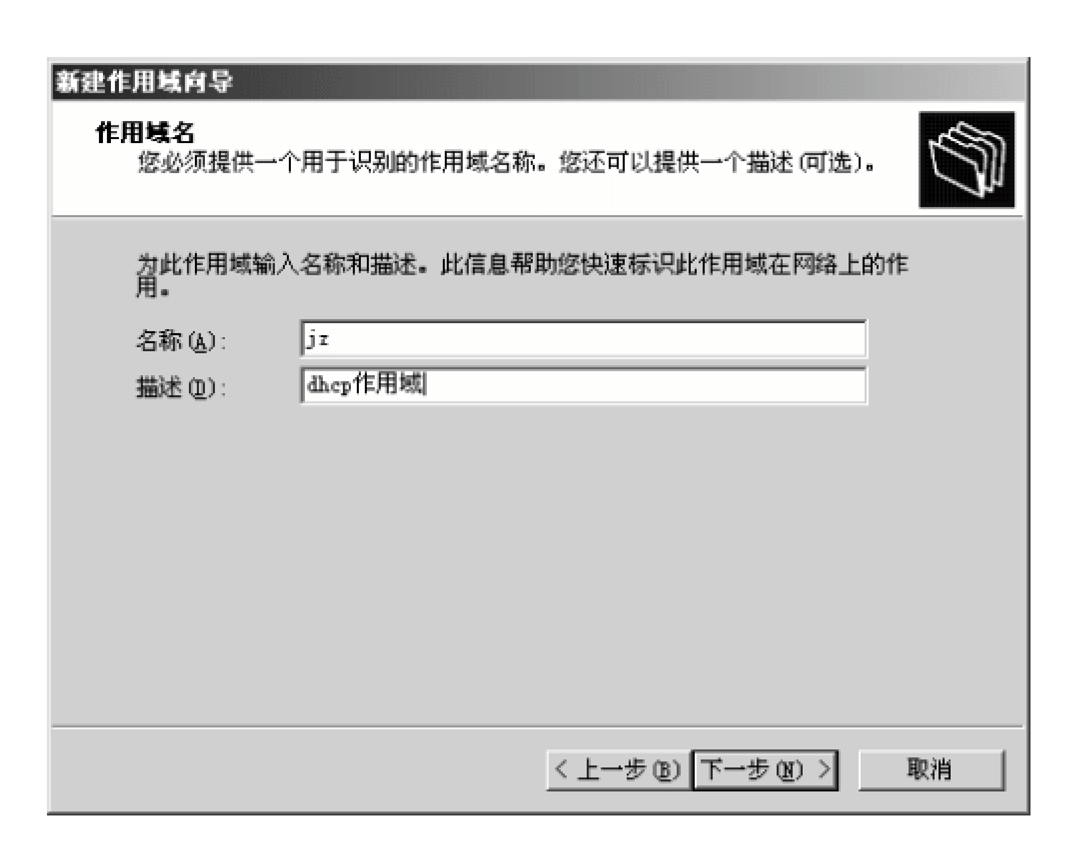


图 3-7　【作用域名】对话框

（3）单击【下一步】按钮，打开如图 3-8 所示的【IP 地址范围】对话框。在其中输入起始 IP 地址为 192.168.20.31，结束 IP 地址为 192.168.20.200，子网掩码为：255.255.255.0。

（4）单击【下一步】按钮，打开如图 3-9 所示的【添加排除】对话框。在其中输入排除的地址范围（不能分配的 IP 地址），起始 IP 地址为 192.168.20.101，结束 IP 地址为 192.168.20.110，单击【添加】按钮。

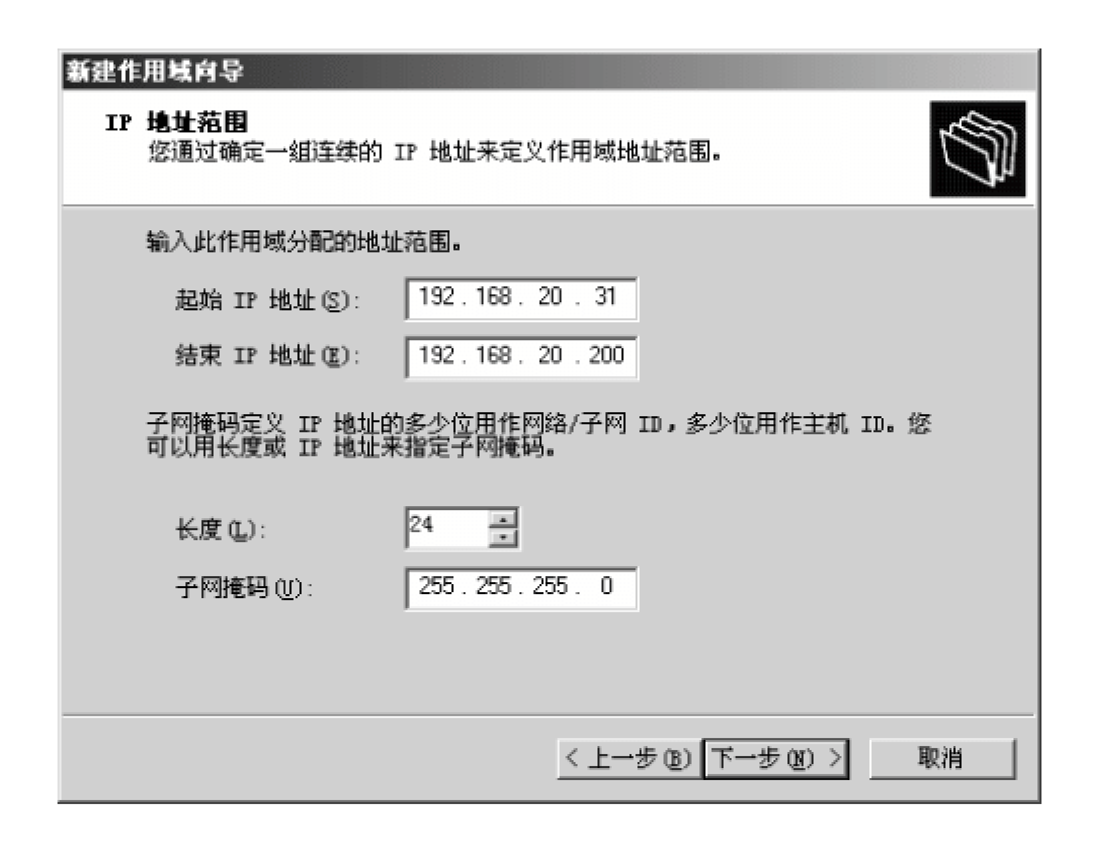


图 3-8　【IP 地址范围】对话框

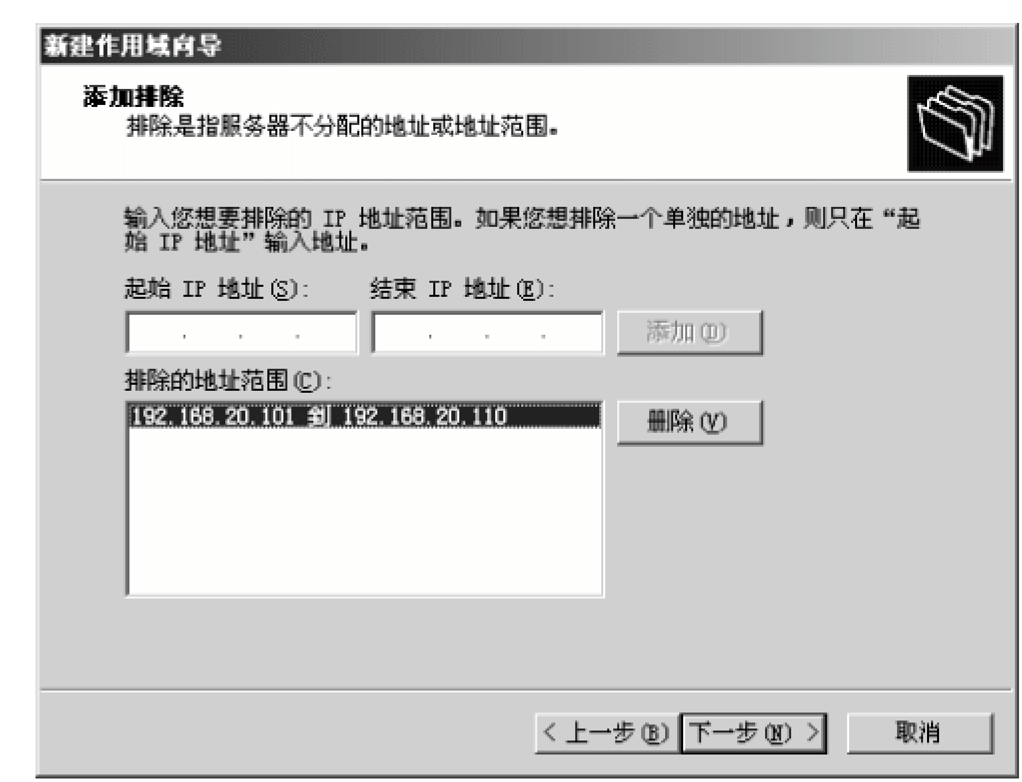


图 3-9　【添加排除】对话框

（5）单击【下一步】按钮，打开如图 3-10 所示的【租约期限】对话框。在其中输入租约期限。



(6) 单击【下一步】按钮，打开【配置 DHCP 选项】对话框。在其中选择【是，我想现在配置这些选项】单选按钮。

(7) 单击【下一步】按钮，打开如图 3-11 所示的【路由器(默认网关)】对话框。在其中输入路由器的 IP 地址为 192.168.20.1，单击【添加】按钮，可添加多个。



图 3-10 【租约期限】对话框



图 3-11 【路由器(默认网关)】对话框

(8) 单击【下一步】按钮，打开如图 3-12 所示的【域名称和 DNS 服务器】对话框。在其中输入 DNS 服务器的 IP 地址为 192.168.20.11，单击【添加】按钮，可添加多个。

(9) 单击【下一步】按钮，打开如图 3-13 所示的【WINS 服务器】对话框。在其中输入 WINS 服务器的 IP 地址为 192.168.20.12，单击【添加】按钮，可添加多个。

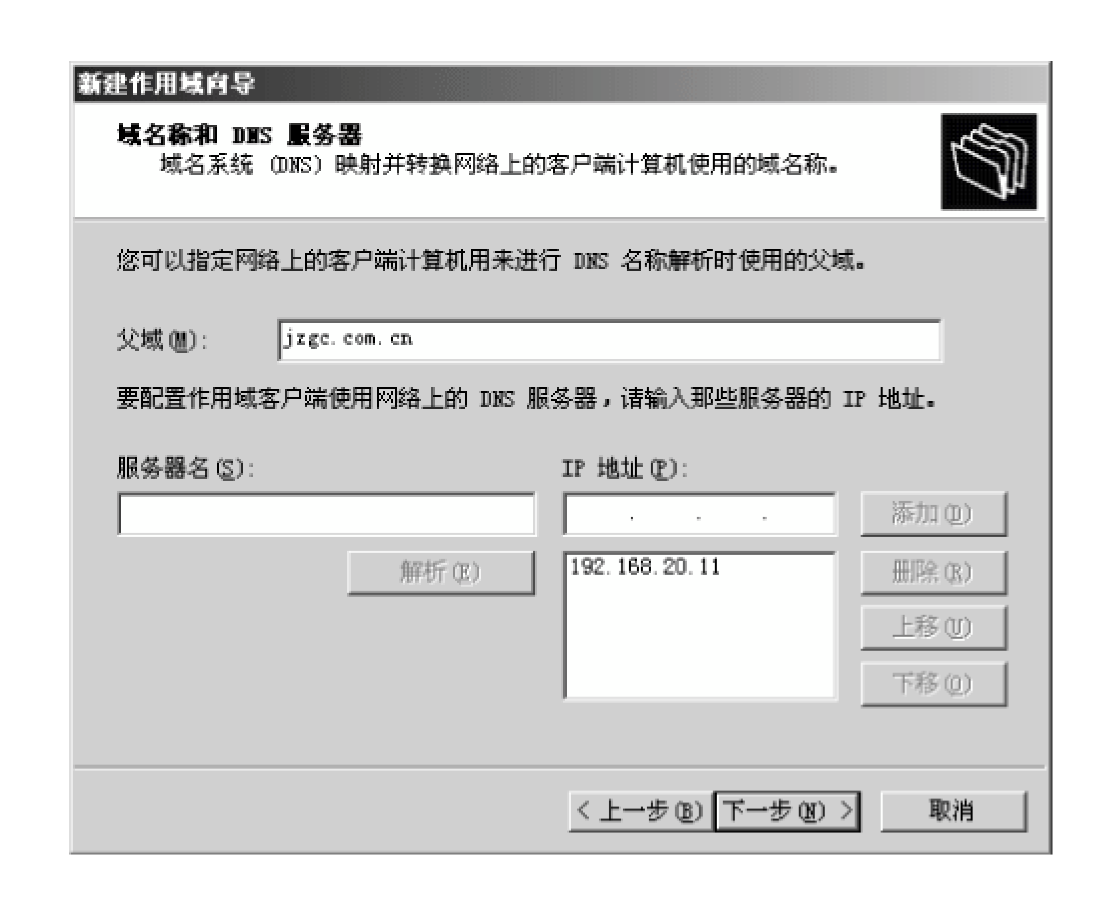


图 3-12 【域名称和 DNS 服务器】对话框

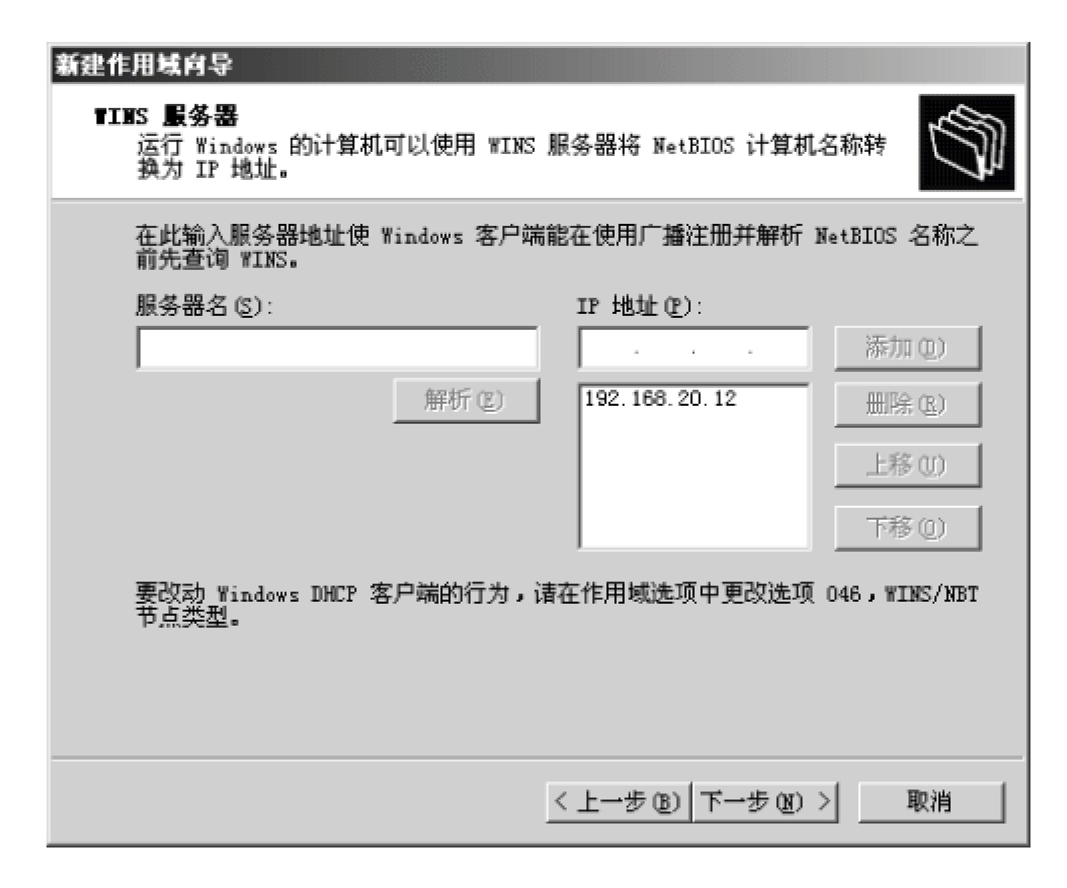


图 3-13 【WINS 服务器】对话框

(10) 单击【下一步】按钮，打开【激活作用域】对话框。在其中选择【是，我想现在激活此作用域】单选按钮。

(11) 单击【下一步】按钮，在之后出现的对话框中单击【完成】按钮。至此，创建 DHCP 作用域完成，如图 3-14 所示。



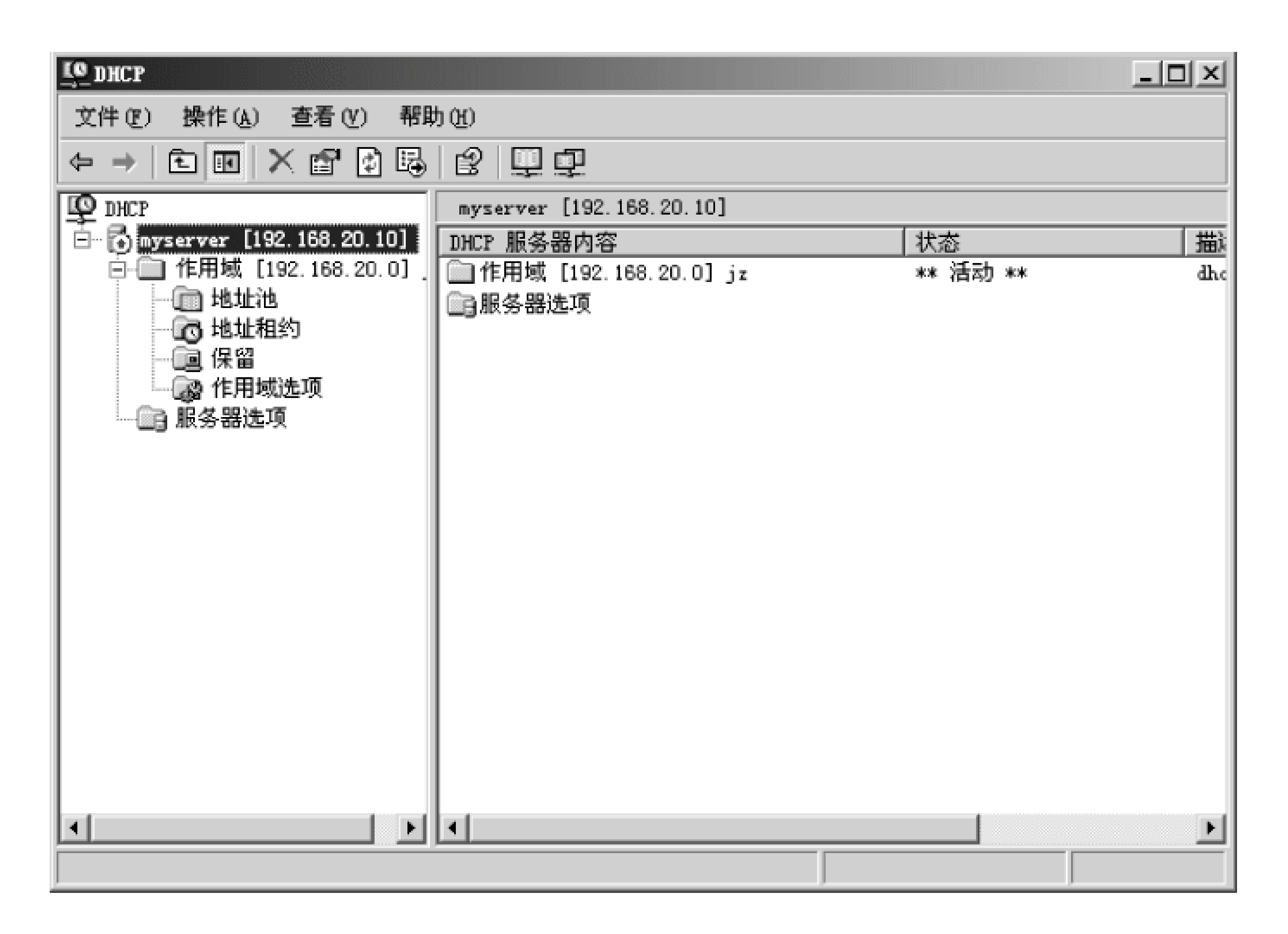


图 3-14　DHCP 作用域创建完成

3.4.2　设置保留地址

如果作用域中的某台主机要作为服务器为其他用户提供网络服务(如 WWW 服务、DNS 服务、FTP 服务),这时 IP 地址最好能够固定。可以把它们的 IP 地址设为静态 IP 而不用动态 IP,此外也可以让 DHCP 服务器为它分配固定的 IP 地址。

通过使用保留,可以为某个特定 MAC 地址的 DHCP 客户端保留一个特定的 IP 地址,此时保留的 IP 地址将不会用于为其他 DHCP 客户端进行分配。每次当此特定的 DHCP 客户端向此 DHCP 服务器获取 IP 地址时,此 DHCP 服务器总是会将保留的 IP 地址分配给它。设置保留地址的过程如下:

(1) 在 DHCP 控制台中展开某作用域,右击其中的保留项,从弹出的快捷菜单中选择【新建保留】命令,打开如图 3-15 所示的【新建保留】对话框。

(2) 在【保留名称】文本框中指定保留的标识名称,在【IP 地址】文本框中输入要为客户机保留的 IP 地址,在【MAC 地址】文本框中输入客户机网卡的 MAC 编号,最后选择所支持的客户机类型。



图 3-15　【新建保留】对话框

3.4.3　设置 DHCP 选项

除了为 DHCP 客户机动态分配 IP 地址外,还可以利用 DHCP 服务器设置 DHCP 客户机的工作环境,如默认网关、WINS 服务器和 DNS 服务器等,使 DHCP 客户机在启动或更新租约时,自动设置 TCP/IP 环境,从而简化客户端的 TCP/IP 的设置,也便于整个网络的统一管理。例如,在 DHCP 选项设置定义了默认网关为 192.168.20.1,网络中每台启用



DHCP 功能的客户机，默认网关也自动设置为 192.168.20.1。网关地址、DNS 服务器、WINS 服务器等只是常见的几种 DHCP 选项，在 Windows 的 DHCP 服务器中自带了 70 多种 DHCP 选项。DHCP 作用域选项的详细配置过程如下：



图 3-16 【作用域 选项】对话框

(1) 在 DHCP 控制台窗口的目录树中展开相应的作用域。

(2) 右击其中的【作用域选项】节点，从弹出的快捷菜单中选择【配置选项】命令，打开如图 3-16 所示的【作用域选项】对话框。其中有【常规】和【高级】两个选项卡。

(3) 选择【常规】选项卡，从【可用选项】列表中选择要设置的选项，定义相关的参数。例如，要设置路由器，可在下面的【数据输入】区域显示、添加和修改路由器的 IP 地址，这样 DHCP 客户机自动将路由器信息配置到该机 TCP/IP 设置中(在用新建作用域向导创建作用域时，可直接设置 DNS、路由器和 WINS 这三个选项)。

3.5 DHCP 客户端的设置

DHCP 客户机使用两种不同的过程来与 DHCP 服务器通信并获得配置信息。当客户计算机首先启动并尝试加入网络时，执行初始化过程；在客户机拥有租约之后将执行续订过程，但是需要使用服务器续订该租约。当 DHCP 客户机关闭并在相同的子网上重新启动时，它一般能获得和它关机之前的 IP 地址相同的租约。

3.5.1 配置 DHCP 客户机

与 DHCP 服务器比起来，DHCP 客户机的安装和配置更加简单。详细配置过程如下：

(1) 依次选择【开始】→【设置】→【网络连接】→【本地连接】命令，打开【本地连接状态】对话框。

(2) 在【常规】选项卡的【此连接使用下列项目】列表框中，双击【Internet 协议(TCP/IP)】，打开如图 3-17 所示的【Internet 协议(TCP/IP)属性】对话框。

(3) 选中【常规】选项卡，选中【自动获得 IP 地址】单选按钮，单击【确定】按钮。

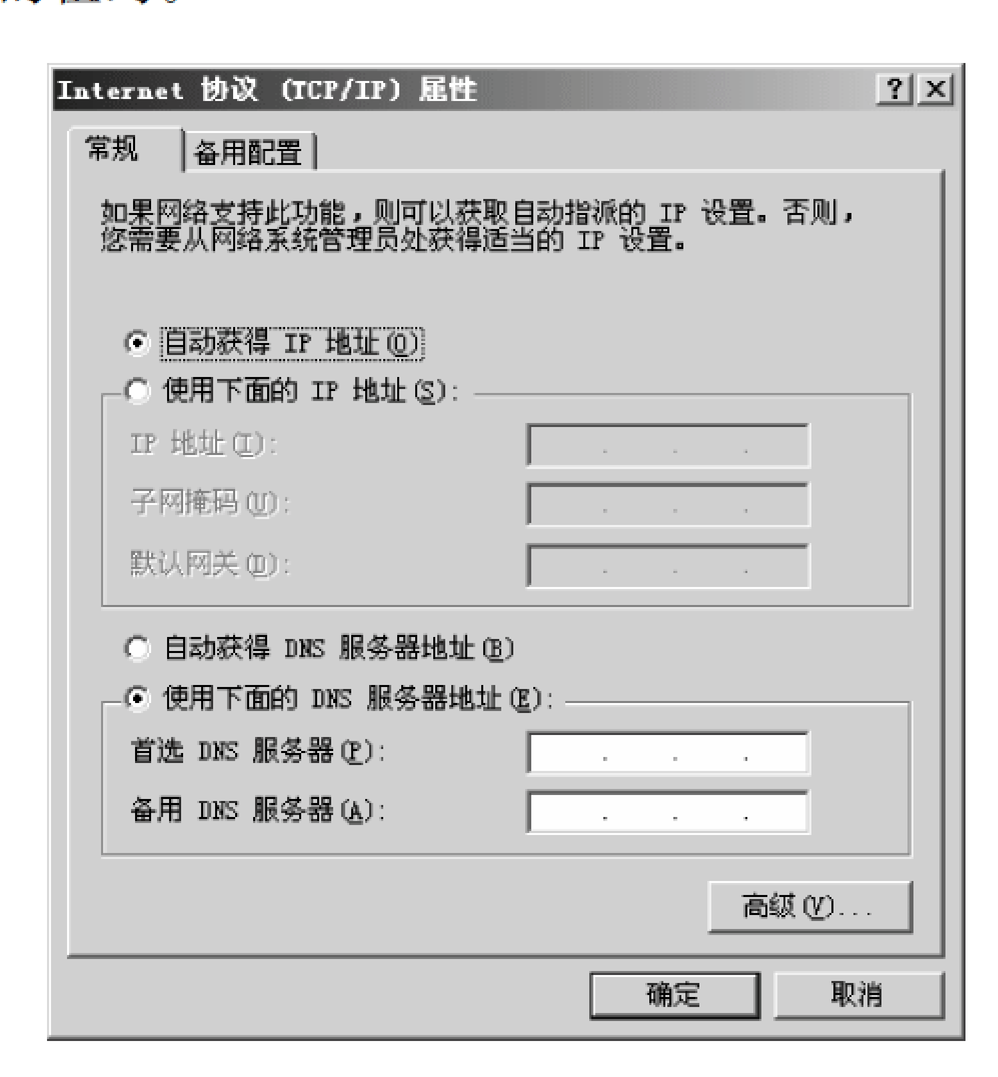


图 3-17 【Internet 协议(TCP/IP)属性】对话框



3.5.2　对 DHCP 进行检测

可以通过如下过程检测 DHCP 客户机是否成功获得了服务器提供的 IP 地址：

(1) 客户端无论是 Windows 2003，还是 Windows 2000、Windows XP，都需要重新启动，再登录。

(2) 在 MS-DOS 方式下运行命令 ipconfig /all，检查自动获得的 IP 地址是多少、是否在 DHCP 服务器规定的 IP 地址范围内。

3.5.3　DHCP 客户机续租地址和释放租约

在租约过期时 DHCP 客户端会释放占用的 IP 地址资源。在租约不过期时，DHCP 客户端也可要求强制更新和释放租约：

(1) 在 MS-DOS 方式下，运行命令 ipconfig /release 来释放现在的 IP 地址。

(2) 在 MS-DOS 方式下，运行命令 ipconfig /renew 来获得新的 IP 地址。

3.6　备份、还原 DHCP 服务器配置信息

服务器往往会由于各种原因而导致系统瘫痪和服务失败，因此，不得不重新安装或恢复服务器。借助定时备份的 DHCP 数据库，就可以在系统恢复后迅速提供网络服务，并减少重新配置 DHCP 服务的难度。备份和还原 DHCP 服务器的过程如下：在 DHCP 控制台窗口中，右击 DHCP 服务器，从弹出的快捷菜单中选择【备份】或者【还原】命令，在打开的对话框里选择要备份或还原文件的路径名，单击【确定】按钮。

3.7　疑 难 解 答

(1) 安装 DHCP 服务器后，如果 DHCP 控制台的目录树中，没有想要管理的 DHCP 服务器应该如何添加一台 DHCP 服务器？

在 DHCP 控制台的目录树中，右击 DHCP 根节点，从弹出的快捷菜单中选择【连接到 DHCP 服务器】命令，在打开的【连接到 DHCP 服务器】对话框中选择【这台计算机】单选按钮，把本地的这台计算机作为 DHCP 服务器进行管理，或者选择【下列计算机】单选按钮，在下面的文本框中输入需要管理的某台 DHCP 服务器的名字或 IP 地址来对其进行管理。

(2) 如果 DHCP 作用域中的某台主机要作为 WWW 服务器为其他用户提供网络服务，这时应该如何设置 DHCP 服务器让它为 WWW 服务器自动分配 IP 地址？

此时 WWW 服务器的 IP 地址最好能够固定。可以让 DHCP 服务器为它设置保留地址。通过使用保留，可以为 WWW 服务器的 MAC 地址的 DHCP 客户端保留一个特定的 IP 地址，此时保留的 IP 地址将不会用于为其他 DHCP 客户端进行分配。每次当 WWW 服务器向 DHCP 服务器索取 IP 地址时，此 DHCP 服务器总是会将保留的 IP 地址分配给它。



(3) DHCP服务器配置完毕后,如何知道DHCP客户机是否成功地自动获得了DHCP服务器分配的IP地址?

在MS-DOS方式下运行命令ipconfig /all,检查客户机的IP地址是多少、是否在DHCP服务器设置的IP地址池内。

习　　题

1. 填空题

(1) DHCP服务的全称是________。

(2) DHCP服务器在续租某一个正在使用的IP地址时,需要经过________和________两步来完成。

2. 选择题

(1) DHCP除了可以为客户机动态分配IP地址外,还可以设置DHCP客户机的(　　)。

A. 默认网关　　B. DNS服务器　　C. WINS服务器　　D. 以上三项

(2) 可以通过运行(　　)命令来释放现在的IP地址。

A. ipconfig /release　　B. ipconfig /renew

C. ipconfig /all　　D. ipconfig

3. 思考题

(1) DHCP分配IP地址的过程如何?

(2) DHCP允许有哪三种类型的地址分配?

第4章　Web服务器配置与管理

本章要点

- 了解 HTML 语言
- 掌握 IIS 6.0 的安装及配置方法
- 掌握虚拟主机的建立方法
- 了解网站的安全配置方式

网络重在应用，要学习计算机技术，必须熟练掌握各种网络应用知识，熟悉各种各样的服务器平台和网络应用环境。本章将详细介绍 Web 服务器的搭建。

4.1　WWW 服务概述

万维网（World Wide Web，WWW）是一个基于超文本（Hypertext）方式的信息查询工具，其最大特点是拥有友善的图形界面、简单的操作方法以及图文并茂的显示方式。

WWW 系统采用客户机/服务器结构。在客户端，WWW 系统通过 Internet Explorer 等浏览器软件提供查阅超文本的方便手段。在服务器端，定义了一种组织多媒体文件的语言——超文本标记语言（HyperText Markup Language，HTML），按 HTML 格式储存的文件被称做超文本文件。每一个超文本文件中通常都有一些超链接（Hyperlink），把该文件与别的超文本文件连接起来构成一个整体。

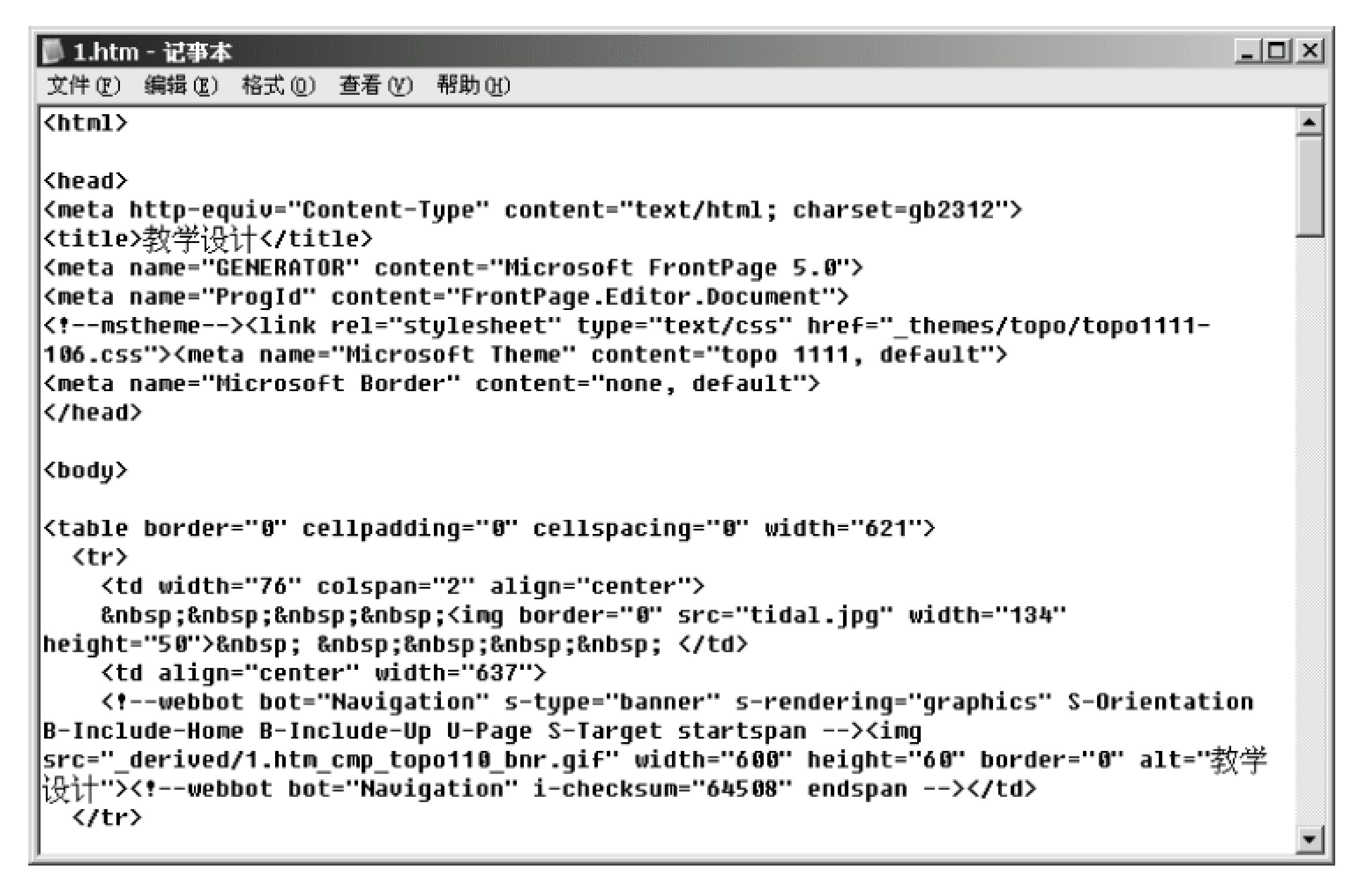
各个网站都是由若干网页组成的，当用户从 Web 服务器得到一个页面后，需要在自己的屏幕上将它正确无误地显示出来。由于将文件放入 Web 服务器的用户并不知道将来阅读这个文件的用户使用何种类型的计算机或者终端，因此要保证每个人在屏幕上都能读到正确显示的文件，就必须以某种各类型的计算机或者终端都能“看懂”的方式来描述文件，即遵循一系列标准，于是就产生了 HTML。

HTML 对 Web 页的内容、格式及 Web 页中的超级链接进行描述，而 Web 浏览器的作用就是读取网站上的 HTML 文档，再根据 HTML 文档中的描述来显示相应的 Web 页面。

HTML 文档本身是文本格式的，用任何一种文本编辑器都可以对它进行编辑，如图 4-1 所示。HTML 语言有一套相当复杂的语法，专门提供给专业人员用来创建 Web 文档，一般用户并不需要掌握它。

仅有 HTML 并不能完成 WWW 服务的全部内容，还需要在网络中传输这些 HTML






```
<html>

<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>教学设计</title>
<meta name="GENERATOR" content="Microsoft FrontPage 5.0">
<meta name="ProgId" content="FrontPage.Editor.Document">
<!--mstheme--><link rel="stylesheet" type="text/css" href="_themes/topo/topo1111-
106.css"><meta name="Microsoft Theme" content="topo 1111, default">
<meta name="Microsoft Border" content="none, default">
</head>

<body>

<table border="0" cellpadding="0" cellspacing="0" width="621">
  <tr>
    <td width="76" colspan="2" align="center">
        <img border="0" src="tidal.jpg" width="134"
height="50">       </td>
    <td align="center" width="637">
    <!--webbot bot="Navigation" s-type="banner" s-rendering="graphics" S-Orientation
B-Include-Home B-Include-Up U-Page S-Target startspan --><img
src="_derived/1.htm_cmp_topo110_bnr.gif" width="600" height="60" border="0" alt="教学
设计"><!--webbot bot="Navigation" i-checksum="64508" endspan --></td>
  </tr>
```

图 4-1　HTML 文档源文件

代码,这项工作是由 HTTP(超文本传输协议)完成的。HTTP 是一种应用层协议,它处于 TCP/IP 协议栈的最高层,具体定义了如何利用低层的通信协议完成无错的网络传输,从而在 Web 服务器与浏览器之间建立连接。

4.2　IIS 6.0 服务器的安装和基本管理

IIS 是 Internet Information Services 的简称,就是常说的 Internet 信息服务。它是 Windows Server 2003 的一个重要服务器组件,任何规模的组织都可以使用 IIS 构建和管理 Internet 或 Intranet 上的 Web 网站及 FTP 站点。使用 NNTP(网络新闻传输协议)传输新闻,使用 SMTP(简单邮件传输协议)传输邮件。IIS 6.0 充分利用了最新的 Web 技术标准,可以通过 ASP.NET、XML(可扩展标记语言)来开发、实施和管理 Web 应用程序。

IIS 6.0 的子组件主要有:

- ASP.NET。允许此计算机运行 ASP.NET 应用程序。
- 启用网络 COM+访问。允许此计算机用于主持分布式应用程序的 COM+组件。
- Internet 信息服务管理器。IIS 管理界面的 Microsoft 管理控制台管理单元。
- 万维网服务。IIS 的一个核心组件,使用 HTTP 协议与来自网络上的 Web 客户端交换信息。
- 文件传输协议(FTP)服务。为创建用于上传和下载文件的 FTP 站点提供支持。
- Active Server Pages。用于发布 ASP 文件。

Windows Server 2003 操作系统中,IIS 6.0 作为应用程序服务器的组件出现,默认情况下是没有安装的。可以通过【添加/删除 Windows 组件】来安装。

4.2.1　安装 IIS 信息服务器

一般情况下,Windows Server 2003 服务器默认没有安装 IIS 6.0 组件。因此,IIS 6.0 需要单独安装。



安装步骤如下：

(1) 依次选择【开始】→【设置】→【控制面板】→【添加/删除程序】命令，打开的对话框如图 4-2 所示。



图 4-2　【添加或删除程序】对话框

(2) 在【添加或删除程序】对话框中单击【添加/删除 Windows 组件】图标，会弹出【Windows 组件向导】对话框，如图 4-3 所示。

(3) 在【Windows 组件向导】对话框中选择"应用程序服务器"，单击【详细信息】按钮，从弹出的对话框中选择【Internet 信息服务(IIS)】复选框，然后单击【确定】按钮，如图 4-4 所示。



图 4-3　【Windows 组件向导】对话框

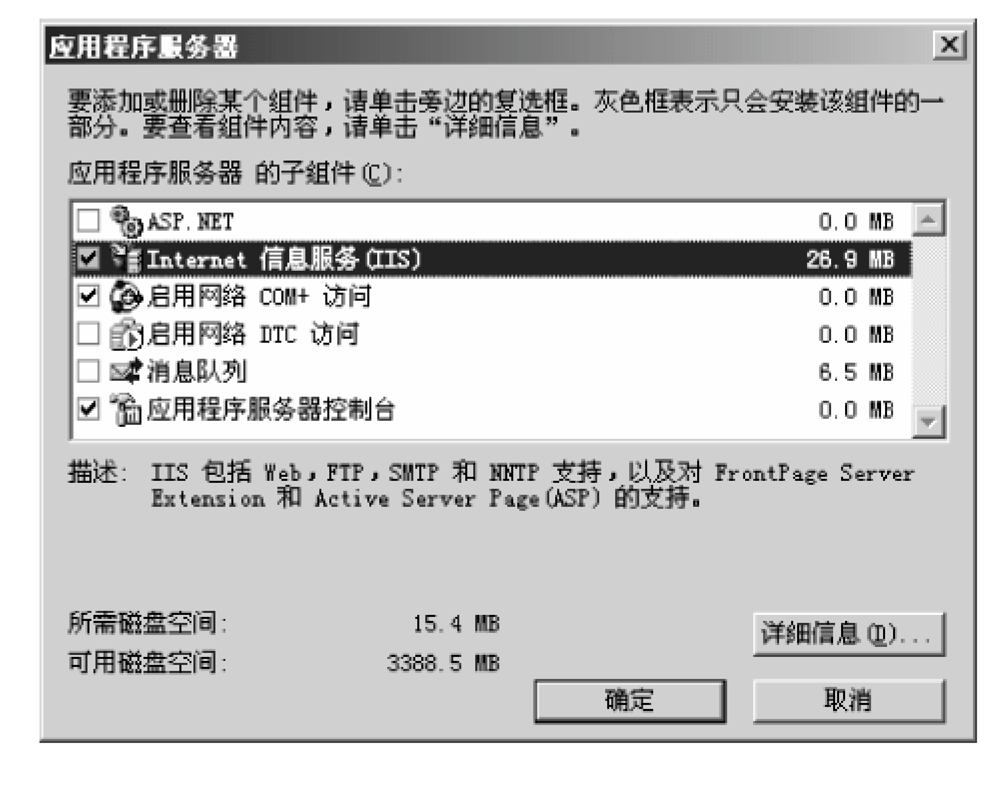


图 4-4　【应用程序服务器】对话框

(4) 安装完毕后，依次选择【开始】→【设置】→【控制面板】→【管理工具】→【Internet 信息服务(IIS)管理器】命令，就会出现如图 4-5 所示的【Internet 信息服务(IIS)管理器】对话框。





图 4-5 【Internet 信息服务(IIS)管理器】对话框

(5) 在 IE 浏览器的地址栏中输入 http://localhost 或者"http://你的计算机名字" 或者 http://127.0.0.1,按 Enter 键后,如果出现如图 4-6 所示界面,则表示 IIS 安装成功。

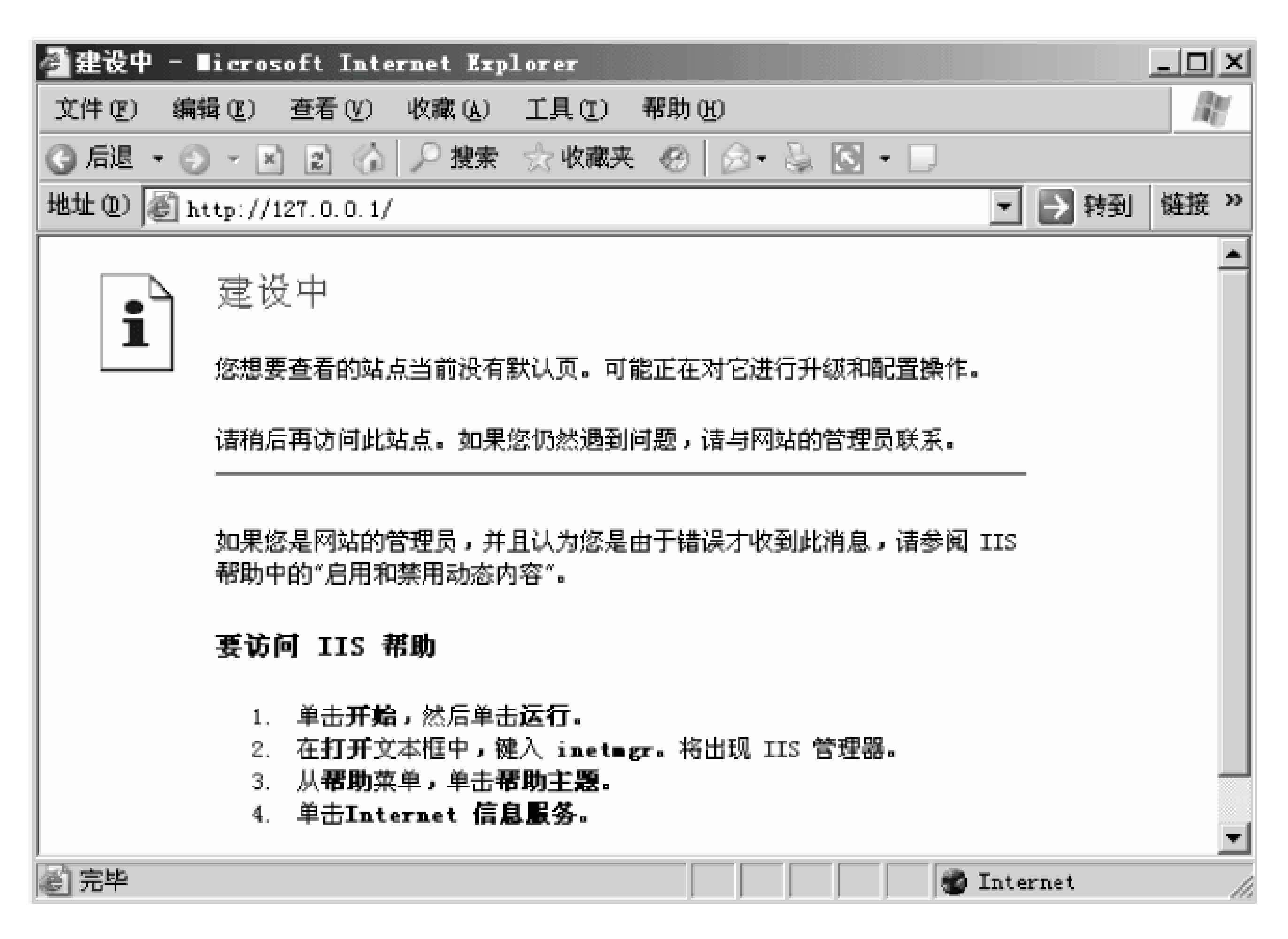


图 4-6 成功安装 IIS

4.2.2 实现远程管理

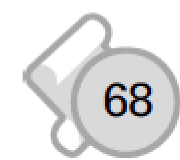
Windows Server 2003 操作系统对服务器有以下两种不同的远程管理方式。

1. 终端+远程桌面连接

这种方式主要用于网络管理员在自己固定的工作站上对服务器进行管理,管理快速、安全,与坐在服务器前操作没有区别。实现方法如下:

(1) 在 Windows Server 2003 中,依次选择【控制面板】→【添加/删除程序】→【添加/删除 Windows 组件】命令,从打开的【Windows 组件向导】对话框中添加"终端服务器"及"终端服务器授权",并且按照默认方式安装。安装完成之后,重新启动服务器。

(2) 从【管理工具】中运行【终端服务器授权】程序,右击计算机名,从弹出的快捷菜单中选择【激活服务器】命令,按照后面的步骤,激活终端服务器。



（3）运行安装后的【远程桌面连接】程序，如图 4-7 所示。

在图 4-7 中单击【选项】按钮，打开【远程桌面连接】的所有选项进行设置，如图 4-8 所示。



图 4-7 【远程桌面连接】对话框

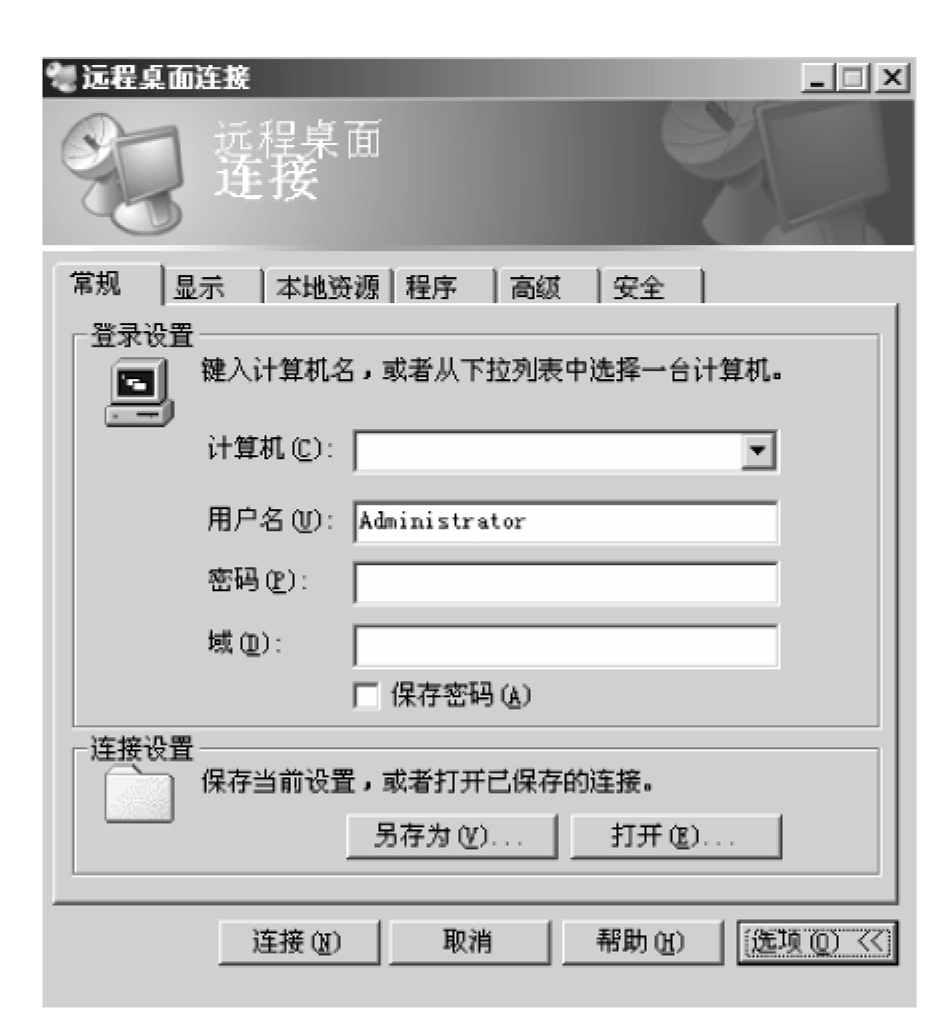


图 4-8 设置远程桌面连接选项

在图 4-8 所示的【计算机】文本框中输入 Windows Server 2003 终端服务器的 IP 地址，在【用户名】文本框中输入管理员账号，在【密码】文本框中输入该账号的密码，并选中【保存密码】复选框。

设置完成后，单击【另存为】按钮，将当前设置保存到一个配置文件中，如命名为 windows2003-1.rdp 文件。以后可以直接双击这个配置文件来调用远程桌面连接程序，并按照当前的配置登录到终端服务器。

2. 远程管理（HTML）

远程管理（HTML）方式，主要用于通过 Internet 对终端服务器进行管理，它具有安全、方便等特点。

当系统管理员在外地或者在家里需要管理服务器时，可能有时找不到“远程桌面连接”程序组件，而采用远程桌面 Web 连接又不是很安全。因此，Windows Server 2003 就提供了一种不需要终端服务器的、安全的 Web 连接方式进行远程管理，即远程管理（HTML）方式。远程管理（HTML）需要使用安全连接，默认端口是 8098，需要输入管理员账户及密码才能登录。实现方法如下。

（1）运行控制面板中的【添加/删除程序】对话框中的【添加/删除 Windows 组件】，依次进入【应用程序服务器】→【Internet 信息服务（IIS）】→【万维网服务】对话框，选择【远程管理（HTML）】复选框之后，按照默认的方式进行安装，如图 4-9 所示。

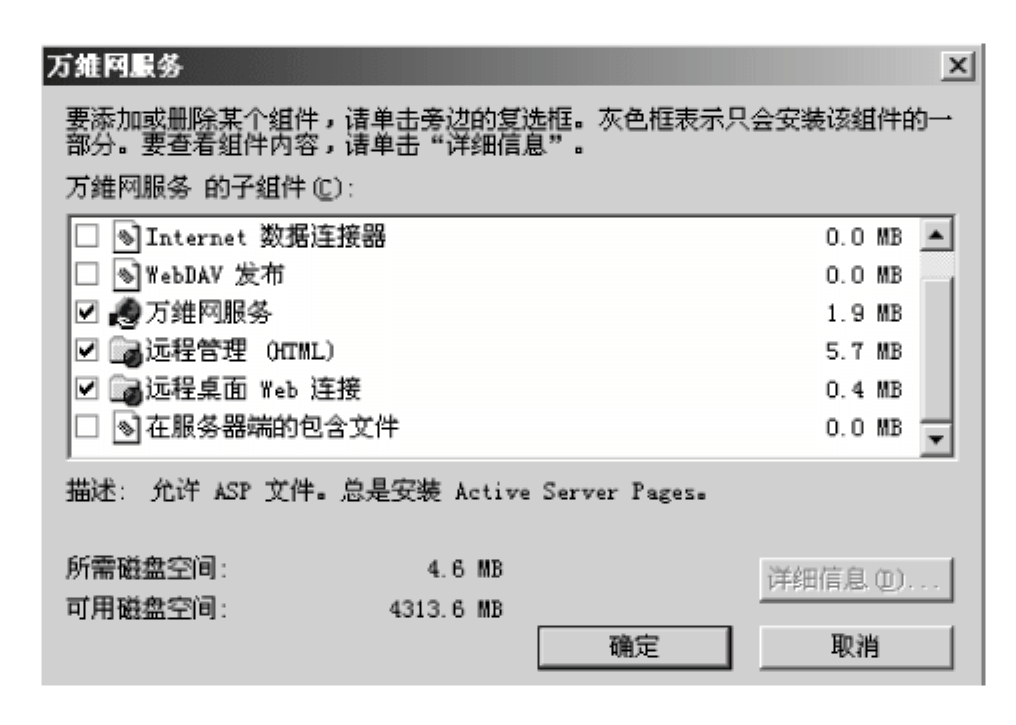


图 4-9 【万维网服务】对话框



（2）在IE浏览器的地址栏中输入https://127.0.0.1:8098，然后根据屏幕提示输入用户名和密码即可登录。登录后远程【服务管理】界面如图4-10所示。



图4-10　远程【服务管理】界面

远程【服务管理】界面提供了【状态】、【站点】、【Web服务器】、【网络】、【用户】、【维护】等选项卡，供管理员管理和维护服务器。要新建或维护站点，可选择【站点】选项卡。完成管理后，管理员可直接关闭IE浏览器，因为是使用安全的Web连接方式。从理论上来说，使用这种连接不会被监听，也不会被记录与跟踪，即使在公共场所对服务器进行管理，也不用担心安全问题。

4.2.3　备份和恢复Web站点

为了保证在网站出现问题时，数据损失最少，并能及时恢复，管理员应该养成经常备份网站的习惯。

1. 站点的备份

管理员可以一次备份一个站点，也可以一次备份整个网站。备份时首先打开【Internet信息服务(IIS)管理器】。要备份整个网站，可右击【网站】，在弹出的快捷菜单中依次选择【所有任务】→【将配置保存到一个文件】命令，打开【将配置保存到一个文件】对话框。根据向导提示，完成备份操作。

2. 站点的恢复

在恢复站点时，管理员一次只能恢复一个站点。操作时首先打开【Internet信息服务(IIS)管理器】，右击【网站】，在弹出的快捷菜单中依次选择【新建】→【网站(来自文件)】命令，打开【导入配置】对话框。然后根据提示，即可完成站点恢复操作。



4.3　Web 网站的管理和配置

4.3.1　基本 Web 站点的配置

Web 站点的基本配置步骤如下：

(1) 依次选择【开始】→【设置】→【控制面板】→【管理工具】→【Internet 信息服务(IIS)管理器】命令，展开【ZHL(本地计算机)】，然后展开【网站】。

(2) 右击【默认网站】，从弹出的快捷菜单中选择【属性】命令，打开的对话框如图 4-11 所示。

(3) 选择【网站】选项卡。在【描述】文本框中输入网站名称“默认网站”，在【IP 地址】文本框中输入计算机的 IP 地址 127.0.0.1。

(4) 选择【性能】选项卡，从中设置网站可使用的带宽和 Web 连接数量，如图 4-12 所示。

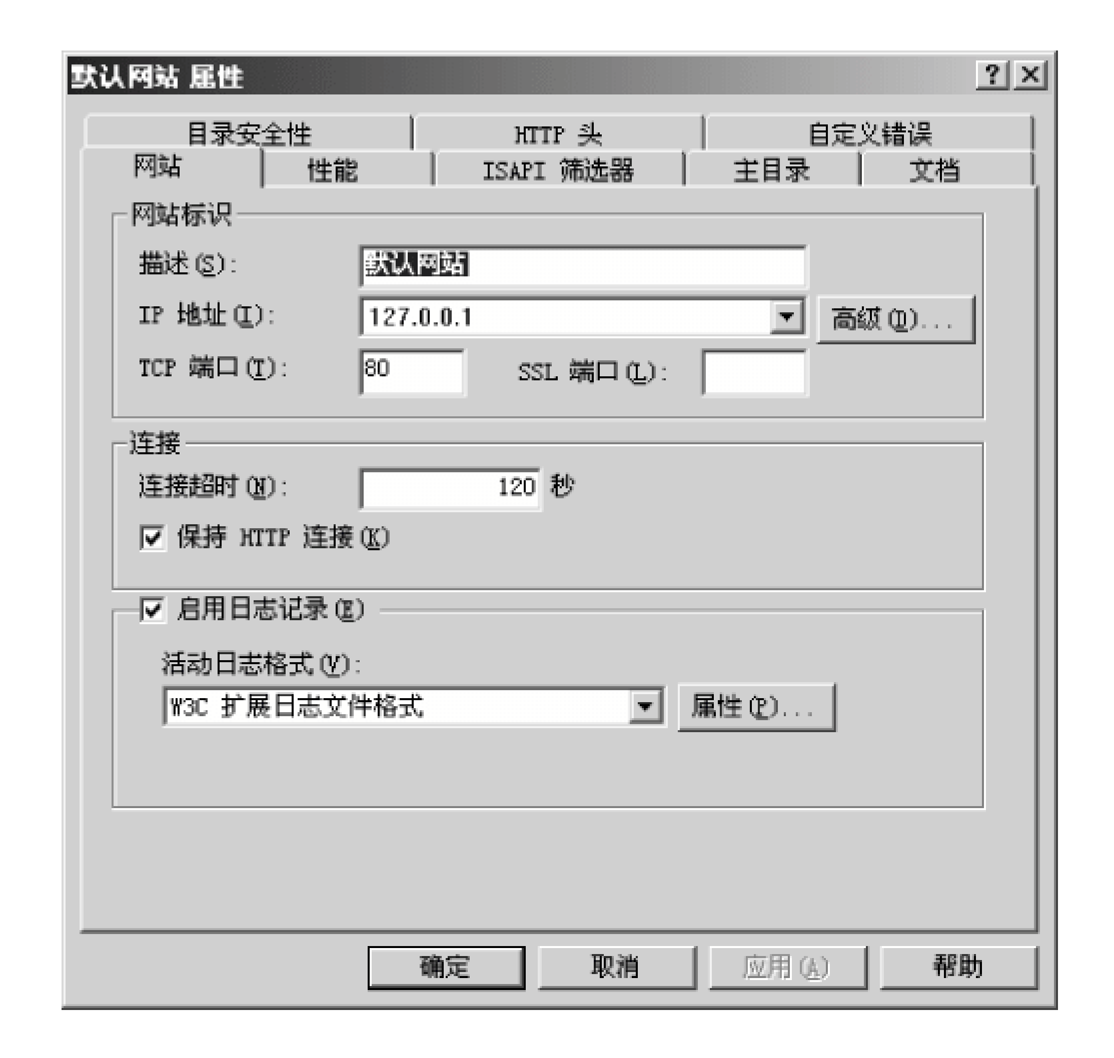



图 4-11　【默认网站 属性】对话框



图 4-12　【性能】选项卡

选中【限制网站可以使用的网络带宽】复选框，可配置 IIS 将网络带宽调节到选定的最大带宽量，以千字节每秒(KB/s)为单位。通过配置某个站点的网络带宽，可以更好地控制访问该站点的通信量。

在【网站连接】选项组中，可选择特定数目或者不限定数目的 Web 服务连接。限制连接可使计算机资源能够用于其他进程。

(5) 选择【主目录】选项卡，如图 4-13 所示。

如果想使用在本地计算机上的网站内容，则选中【此计算机上的目录】单选按钮，然后在【本地路径】文本框中输入本地路径或通过单击【浏览】按钮来选择一个本地路径，如默认路径 C:\inetpub\wwwroot。但为了增加安全性，一般不在默认路径下创建 Web 站点。如果要使用另一台计算机上的 Web 内容，则选中【另一台计算机上的共享】单选按钮，然后在显示的【网络目录】文本框中输入所需位置。如果要使用另一个 Web 站的网页内容，则选中



【重定向到 URL】单选按钮，然后在【重定向到】文本框中输入所需位置。

(6) 选择【文档】选项卡，设置网站的默认启动文档，如图 4-14 所示。如果要使用 example.htm 作为启动文档，就得单击【添加】按钮将其添加到默认文档列表框中。

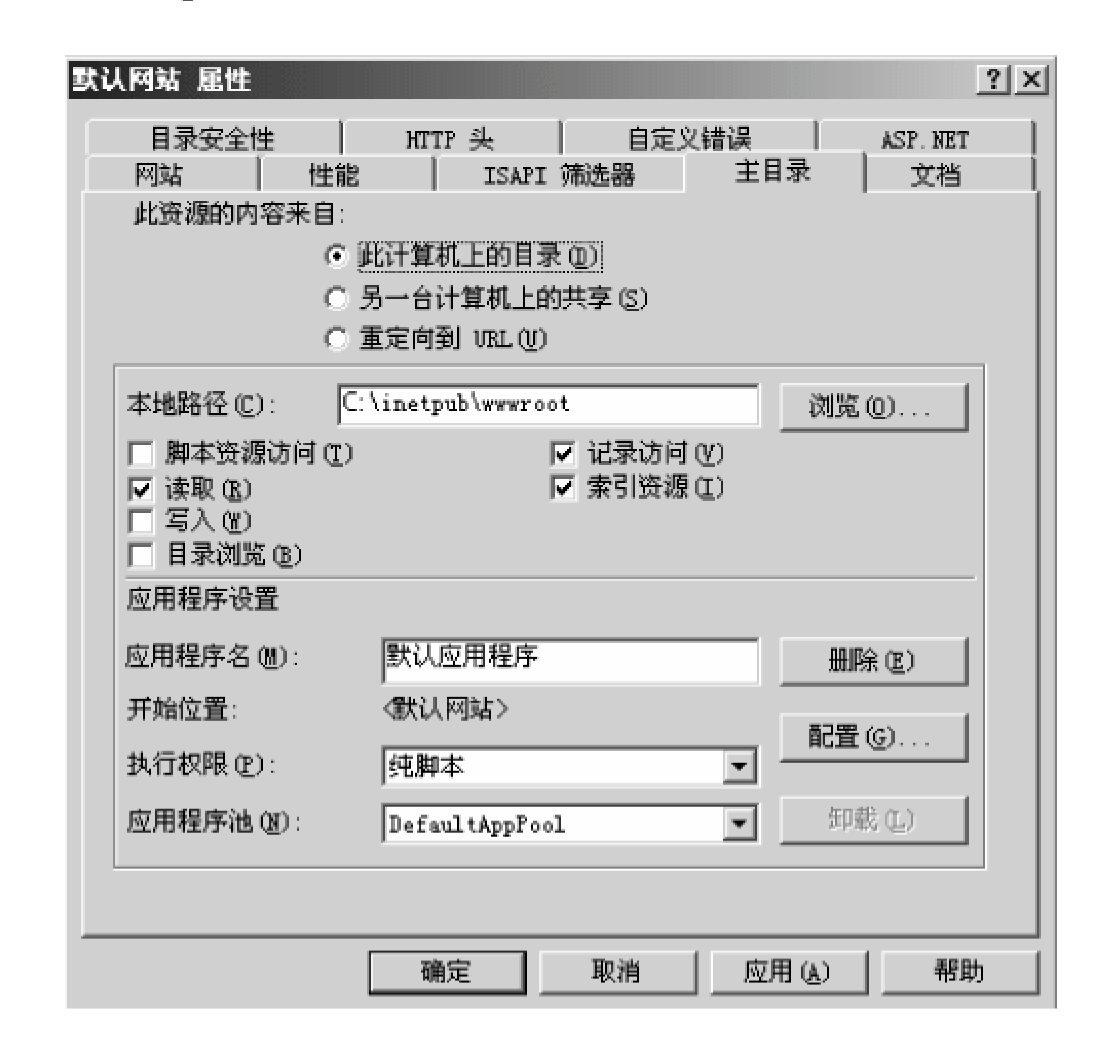


图 4-13 【主目录】选项卡

图 4-14 【文档】选项卡

(7) 单击【确定】按钮，关闭【默认网站属性】对话框，然后单击【确定】按钮，返回到【Internet 信息服务(IIS)管理器】窗口。

此时默认 Web 站点已经启动了。但 IIS 6 默认安装完成后只支持静态页面，不能正常显示基于 ASP 的动态 Web 网页内容，因此打开其动态内容支持功能。在【Internet 信息服务(IIS)管理器】窗口中，在左侧单击【Web 服务扩展】，在右侧将 Active Server Pages 项启用，如图 4-15 所示。

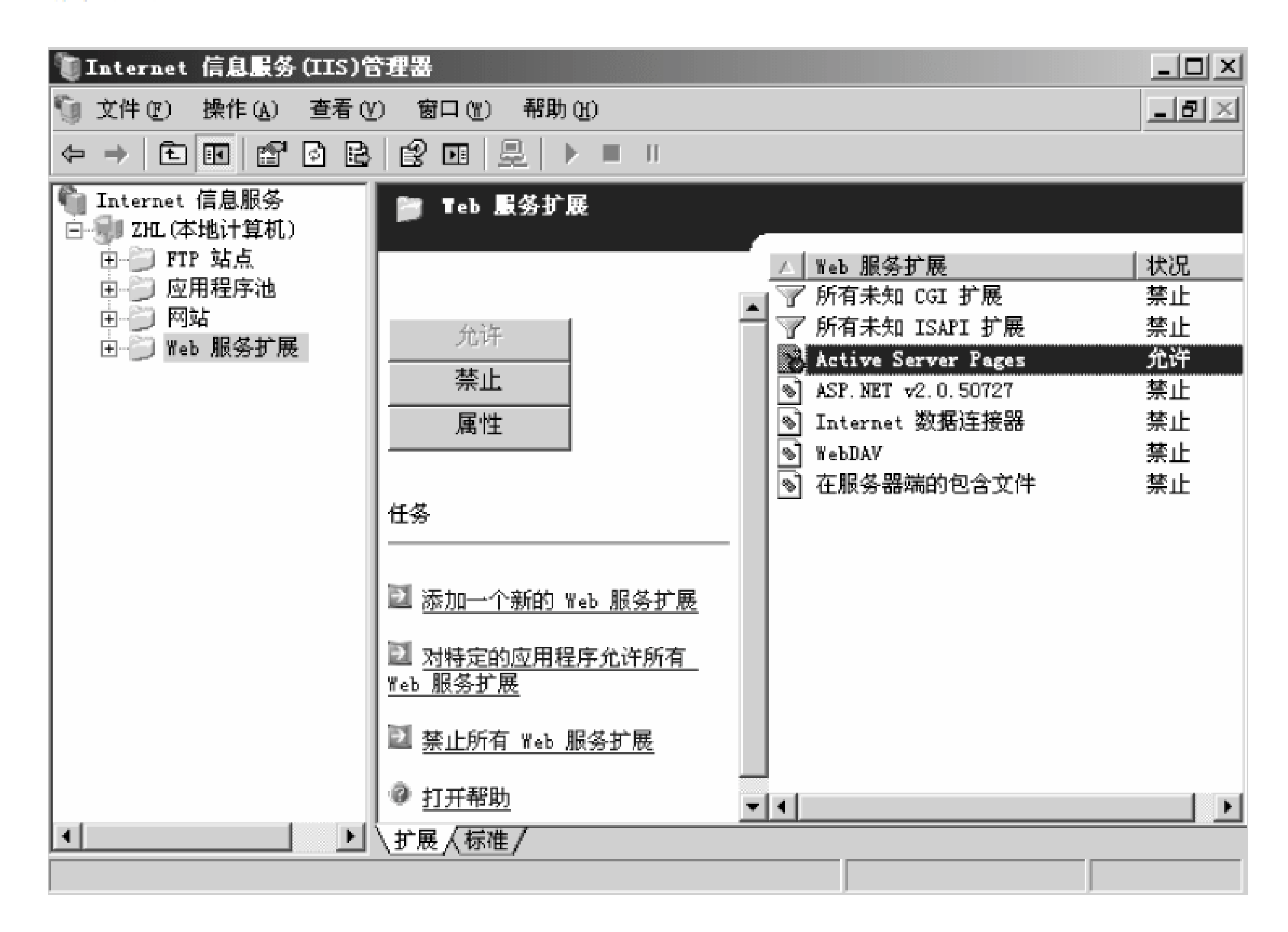


图 4-15 【Internet 信息服务(IIS)管理器】窗口



4.3.2 发布已经制作好的网站

假设已经做好一个网站，存储在本地计算机的“E:\Win2003 书稿”目录中，则可以通过下列操作将这个网站发布到网络上。

(1) 在【Internet 信息服务(IIS)管理器】窗口中，右击【网站】，从弹出的快捷菜单中选择【设置】→【控制面板】命令，打开【网站创建向导】对话框。在【描述】文本框中，根据需要写入对要发布网站的简要描述，然后单击【下一步】按钮，打开【IP 地址和端口设置】对话框。在【网站 IP 地址】列表框中选择分配到的 IP 地址，其他选项使用默认设置，如图 4-16 所示。

(2) 单击【下一步】按钮，打开【网站主目录】对话框。单击【路径】文本框后的【浏览】按钮，选择网站文件所在目录“E:\Win2003 书稿”。然后单击【下一步】按钮，打开【网站访问权限】对话框，一般采用默认设置即可，如图 4-17 所示。

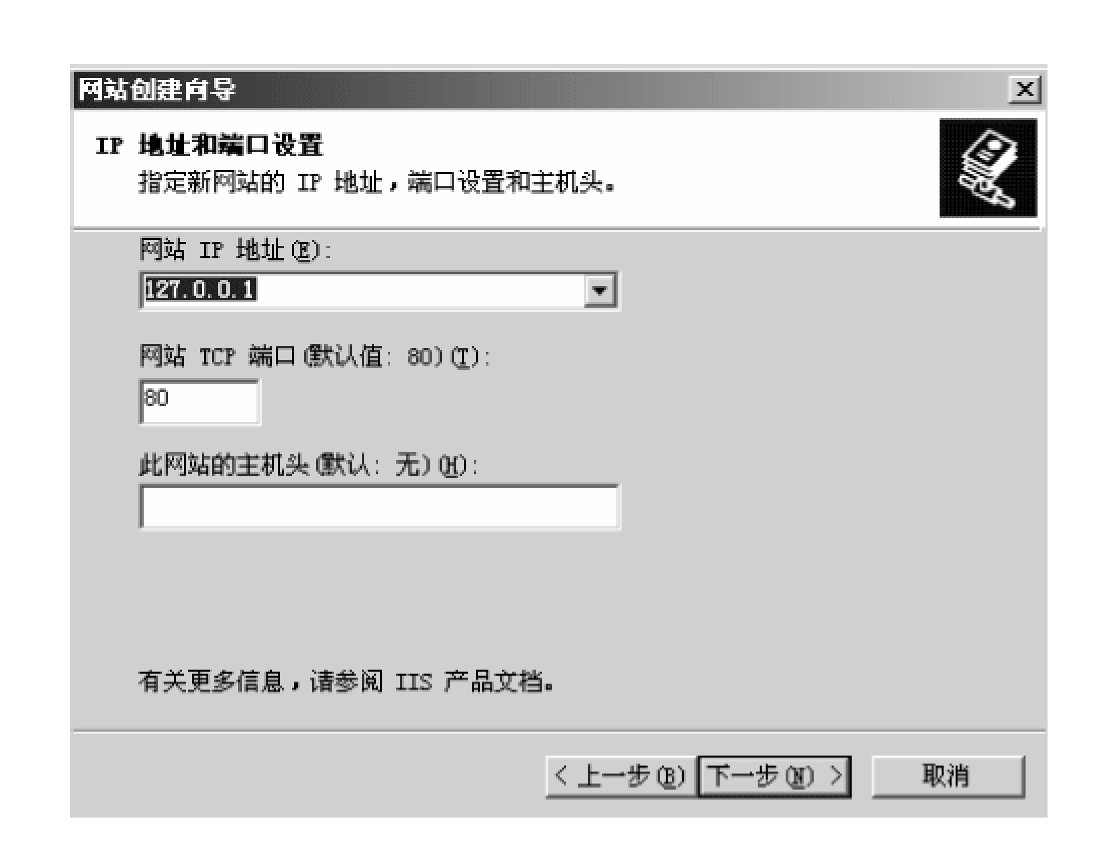


图 4-16 【IP 地址和端口设置】对话框

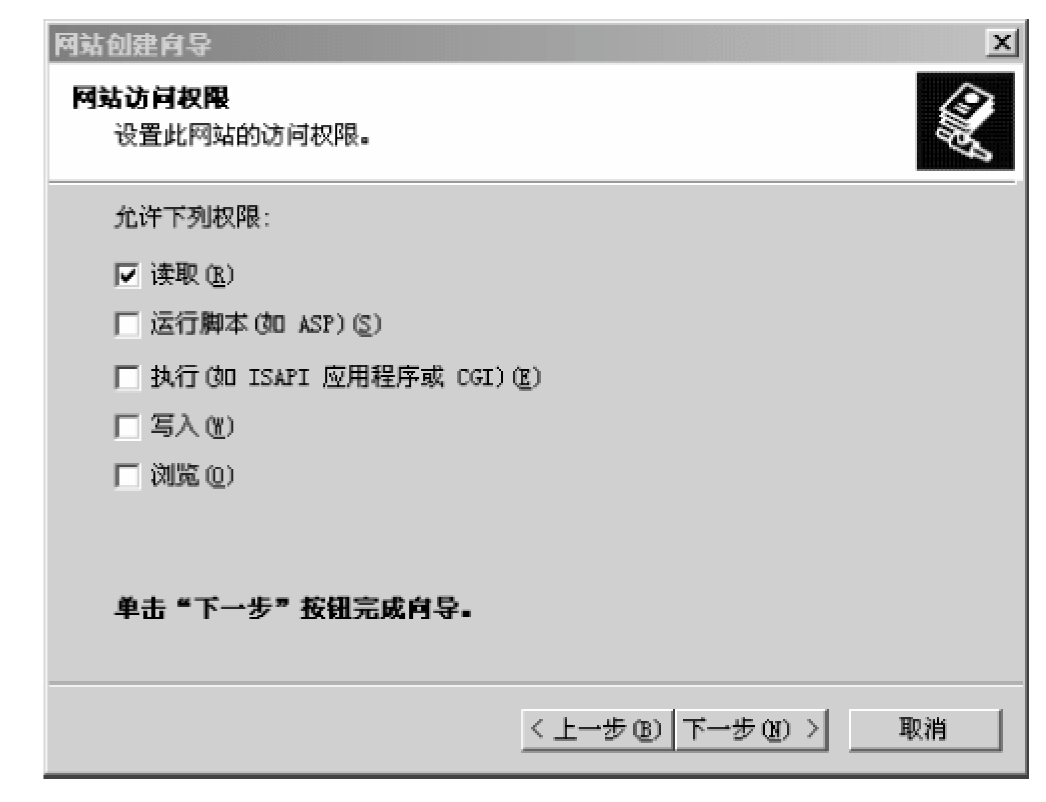


图 4-17 【网站访问权限】对话框

(3) 单击【下一步】按钮，完成网站的发布。

(4) 测试“我的网站”是否正常运行。打开 IE 浏览器，在地址栏中输入网址 http://127.0.0.1 访问“我的网站”。如图 4-18 所示，即表示“我的网站”已经成功发布到网络上。

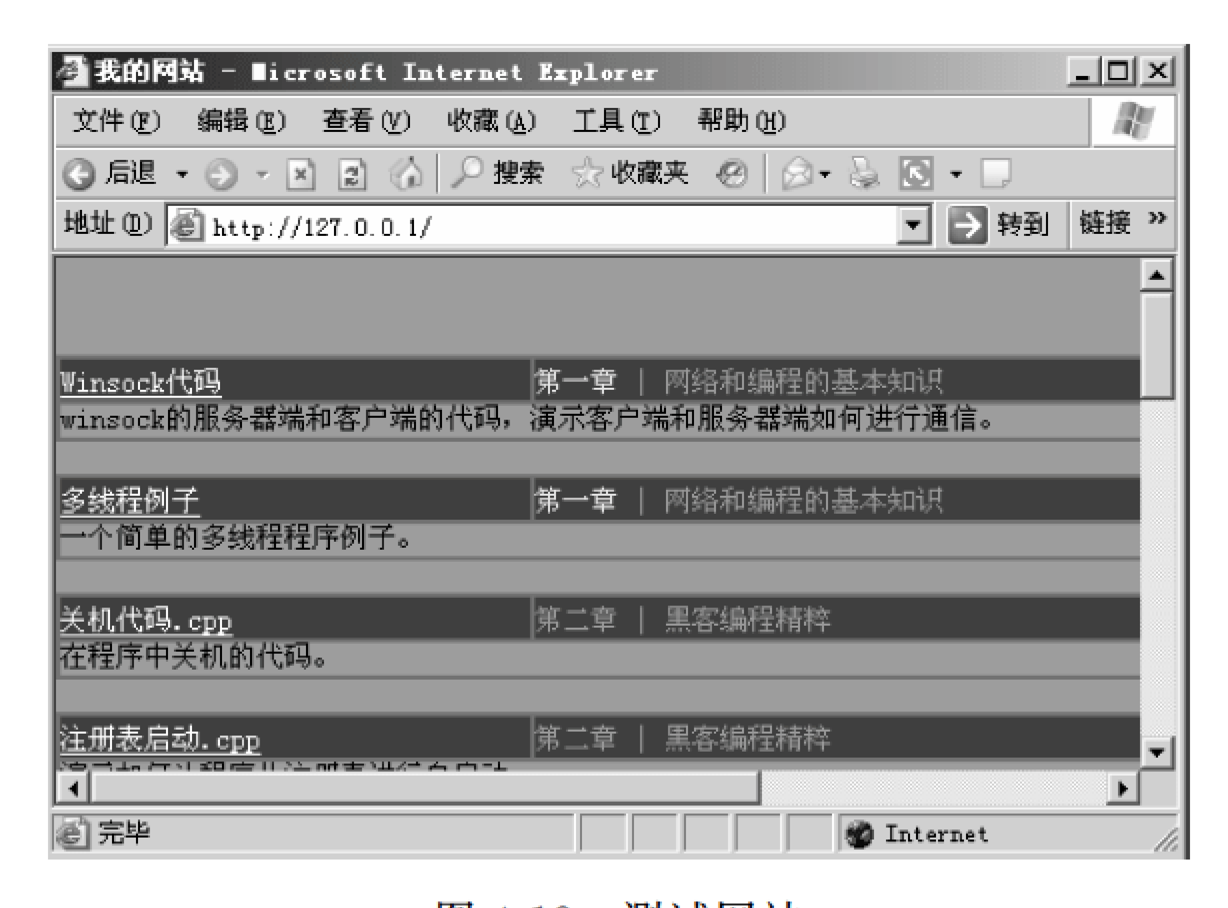


图 4-18 测试网站



4.4 建立虚拟主机

在一台计算机上实现多个 Web 站点的方式称为虚拟服务器或虚拟主机，这样可以极大地节省硬件成本。

一般用域名来标记站点，站点的数量与域名个数相等，并且一个域名往往是与一个 IP 地址对应。这样，服务器拥有的 IP 地址个数应该与虚拟服务器的数量相同，即一个 IP 地址对应一个服务器。但是由于 IP 地址资源的紧缺，管理员往往要借助其他手段在同一 IP 地址上实现多个站点。下面介绍两种常见的虚拟主机实现方式：端口号方式和主机头方式。

4.4.1 端口号方式

TCP 端口号是客户机浏览器与 Web 服务器之间的信息通道，TCP 端口号可以多达五位数。每种网络服务都需要在服务器上指定一个 TCP 端口号，客户机要浏览服务器的内容须在浏览器的地址栏中指定同一端口号。那么，为什么平常上网时不必输入端口号呢？这是因为常见的 Internet 服务都拥有默认的端口号。例如，WWW 服务的默认端口为 80，FTP 服务的默认端口为 21。这样在浏览器中输入站点地址时，即使不指定 80 端口，浏览器仍然自动以 80 端口与服务器进行通信。

这样，即使两个站点拥有同样的 IP 地址，但只要给它们指定不同的 TCP 端口就可以将它们区分开来。但是如果将端口号从默认的 80 更改为其他数值，客户机浏览站点内容时必须手工指定使用的端口，即在浏览器地址栏中输入域名后加上“:”和更改后的端口号数值。例如，在同一台服务器上有两个网站 www.test1.com 和 www.test2.com，它们共用一个 IP 地址 192.168.1.30，管理员可以让 www.test1.com 使用默认端口 80，而让 www.test2.com 使用端口 90。这样在浏览器地址栏中输入地址 192.168.1.30 得到的是 www.test1.com，要想访问 www.test2.com 就要输入 192.168.1.30:90。

可以通过下面的操作更改一个网站的端口号：

(1) 打开【IIS 管理环境】，右击管理控制树中要更改端口的站点，从弹出的快捷菜单中选择【属性】命令，调出网站的【属性】对话框。

(2) 在网站的【属性】对话框中选择【网站】选项卡，在【TCP 端口】文本框中输入该网站要使用的新的端口号，然后单击【确定】按钮，完成端口号的设置。

以端口号方式实现虚拟主机的方法并不方便，除了要用户记住端口之外，这样的做法也不太符合网络常规，很难用于正规的商业网站。但是某些单位的内部网站，可以通过更改默认端口号来提高网站安全性，避免网络上的普通用户访问。

4.4.2 主机头方式

主机头(Host Header)是除了 IP 地址和 TCP 端口之外的第三个用于区分站点的标识。这样，对于两个共用同一个 IP 地址且都采用默认端口 80 的站点，只要为它们指定不同的主机头，就可以在网络中将它们区分开。

主机头是在 HTTP 1.1 标准中定义的，因此，对于在 IIS 中使用主机头进行配制的站

点，客户浏览器必须支持 HTTP 1.1 标准才能浏览。为站点添加主机头的方法如下：

(1) 打开【IIS 管理环境】，右击管理控制树中要更改主机头的站点，从弹出的快捷菜单中选择【属性】命令，打开网站的【属性】对话框。

(2) 在网站的【属性】对话框中选择【网站】选项卡，单击【高级】按钮，打开【高级网站标识】对话框。

(3) 在【高级网站标识】对话框中单击【添加】按钮，打开【添加/编辑网站标识】对话框。在该对话框的【IP 地址】下拉列表框中选择 IP 地址，在【TCP 端口】文本框中输入默认端口80，在【主机头值】文本框中输入主机头名称，尽量不要包含空格或其他不兼容字符。然后单击【确定】按钮完成主机头的设置。

重复上述操作，就可以为多个站点指定同一 IP 地址、TCP 端口，只要保证它们的主机头不同就可以了。

主机头方式实现虚拟主机操作方便，易于掌握，也能为客户端的访问提供方便，不需要客户记忆各种端口号，只需在客户浏览器中输入不同的主机头名即可访问相应站点。

4.5　Web 网站的目录管理

一个服务器上的网站对应的目录有两种，一种是网站对应的物理目录，就是站点主目录；另一种是虚拟目录，它对应着一个不属于站点主目录的物理目录。当要发布不在站点主目录中的网页内容时，就可以使用虚拟目录。使用虚拟目录，可以对站点进行重新组织，并且可以简化 URL。

建立虚拟目录时需要设置别名，如图 4-19 所示，Web 浏览器就是使用别名来访问虚拟目录的。使用别名可以为管理员和用户带来许多方便。通常，别名要比目录的路径名短，用户输入时比较方便。另外，因为用户不知道文件的物理位置，所以网站也就更加安全；使用别名，管理员可以很容易地在站点中移动目录，可以在不更改 URL 的条件下更改内容的物理位置。

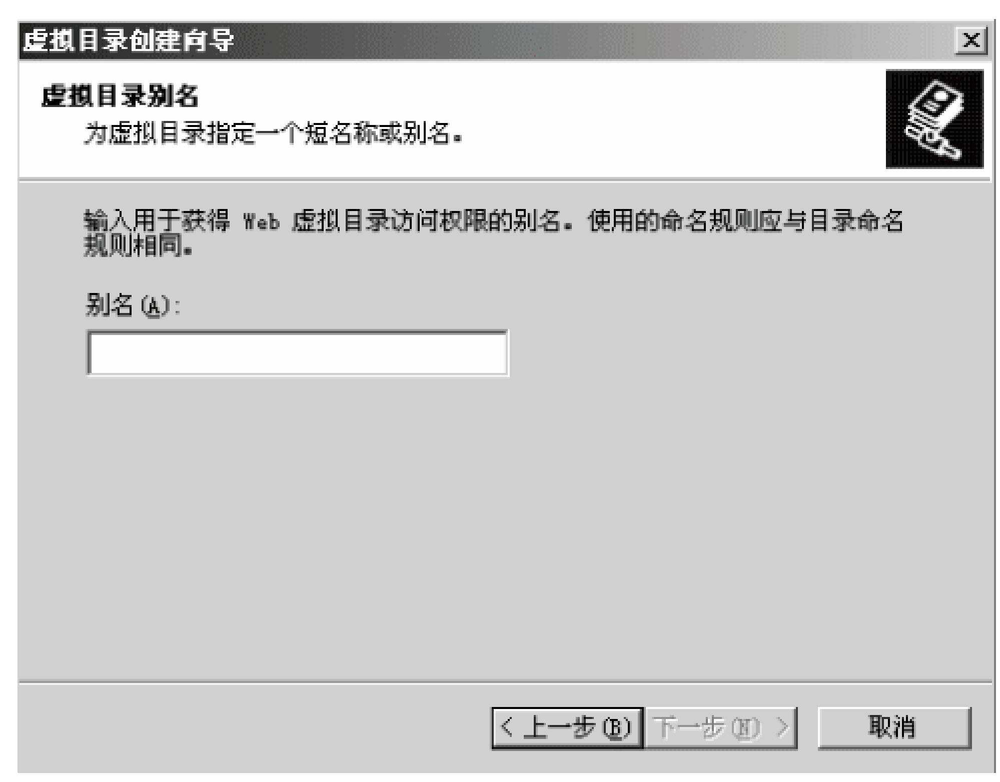


图 4-19　【虚拟目录创建向导】对话框

以本章中的网站为例，站点主目录为“E:\Win2003 书稿”，这个物理目录下有 img 和 inc 两个目录，在 IIS 里可以看到这两个目录。下面来建立一个不属于当前站点主目录“E:\Win2003 书稿”的虚拟目录。

(1) 右击 IIS 目录树的【我的网站】节点，从弹出的快捷菜单中选择【新建】→【虚拟目录】命令，打开【虚拟目录创建向导】对话框，如图 4-19 所示。在【别名】文本框输入虚拟目录的别名，然后单击【下一步】按钮，选择虚拟目录的物理路径，如图 4-20 所示。

(2) 单击【下一步】按钮，设置虚拟目录的访问权限，保持默认即可，这样就完成了虚拟目录的设置。在 IIS 中可以查看到一个图标不一样的目录 download，它就是一个虚拟目录，其物理路径为 D:\download，如图 4-21 所示。



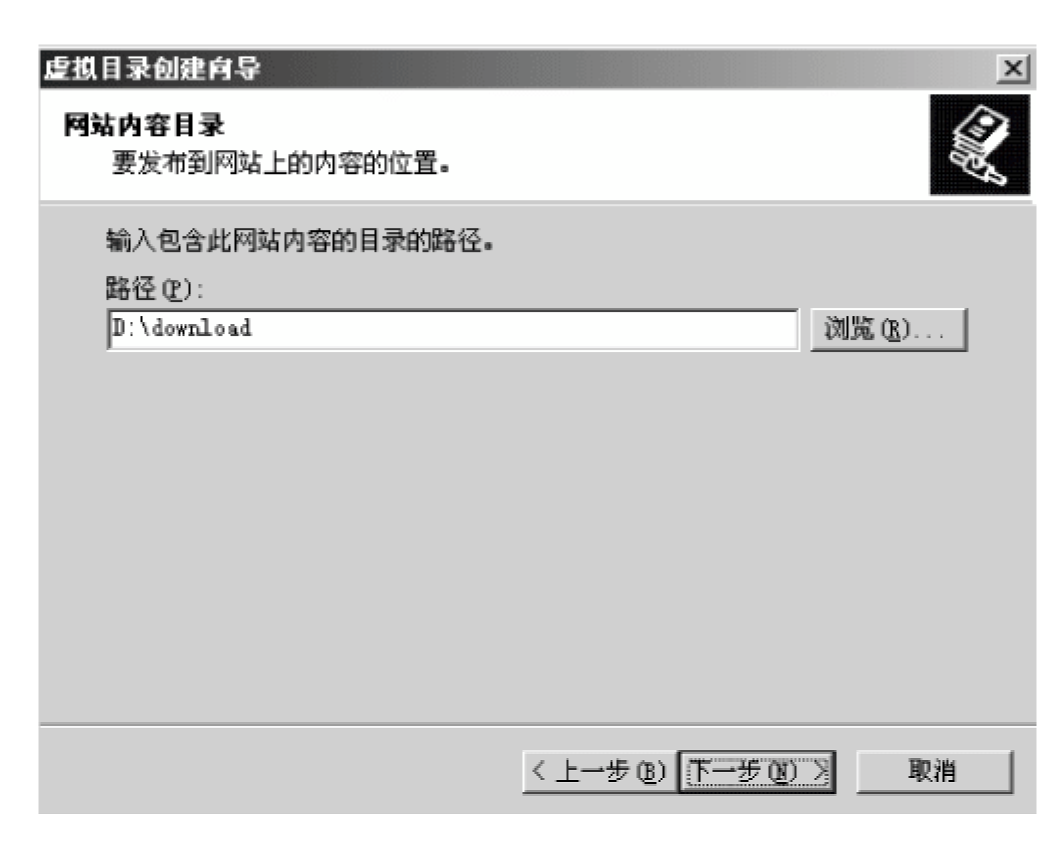


图 4-20 【网站内容目录】对话框



图 4-21 【Internet 信息服务(IIS)管理器】窗口

这样客户浏览的时候，在浏览器的地址栏中输入 http://127.0.0.1/download 就能访问到这个不属于站点主目录下的网页内容。但是用户不知道 download 真正的物理路径，这样可以在一定程度上让网站更安全一些。

4.6 Web 网站安全及实现

影响一个网站安全性的因素很多，主要有网站程序的漏洞、操作系统的漏洞、IIS 的漏洞、日志安全和拒绝服务攻击等。其中网站程序漏洞不在本书讨论范围内，下面主要分析一下其余的 4 个影响因素。

4.6.1 打造安全的操作系统

要创建一个安全可靠的 Web 服务器，必须要实现 Windows 操作系统和 IIS 的双重安全。因为 IIS 用户同时也是 Windows 的用户，并且 IIS 目录的权限依赖 Windows 的 NTFS 文件系统的权限控制，所以保护 IIS 安全的第一步就是确保 Windows 操作系统的安全。一个 Web 服务器可以通过以下方式来增加服务器的安全性。

1. 使用 NTFS 文件系统

在 NT 系统中应该使用 NTFS 系统，NTFS 可以对文件和目录进行权限管理，而 FAT 文件系统只能提供共享级的安全，而且在默认情况下，每建立一个新的共享，所有的用户都能看到，这样不利于系统的安全性。而在 NTFS 文件下，建立新共享后可以通过修改权限保证系统安全。

2. 关闭默认共享

在 Windows 中，有一个“默认共享”，就是在安装服务器的时候，把系统安装分区自动进行共享，虽然对其访问需要管理员的密码，但这是潜在的安全隐患，从服务器的安全考虑，最





好关闭这个“默认共享”，以保证系统安全。方法是更改 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 注册表项，添加键值 AutoShareServer，类型为 REG_DWORD，值为 0。

3. 修改共享权限

在系统默认情况下，每建立一个新的共享，任何用户对该共享目录都有“完全控制”的权限。因此，在建立新的共享后应立即修改 Everyone 的默认权限，不能让 Web 服务器访问者有浏览任意目录的权限，给服务器带来被攻击的危险。

4. 为系统管理员账号改名

对于一般用户，可以在【本地安全策略】的【账户锁定策略】中限制猜测口令的次数，但对系统管理员账号却无法限制，这就可能给非法用户攻击管理员账号口令带来机会，所以需要将管理员账号更名。

5. 禁用 TCP/IP 上的 NetBIOS

NetBIOS 是许多安全缺陷的源泉，所以要禁用它。方法是依次选择【网络邻居】→【属性】→【本地连接】→【属性】命令，打开【本地连接属性】对话框，然后依次选择【Internet 协议(TCP/IP)】→【属性】→【高级】→WINS 命令，选中【禁用 TCP/IP 上的 NetBIOS】单选按钮，如图 4-22 所示。

6. 利用 TCP/IP 筛选

在桌面中依次选择【网络邻居】→【属性】→【本地连接】→【属性】命令，打开【本地连接属性】对话框，选择【Internet 协议(TCP/IP)】→【属性】→【高级】命令，在列表中选中【TCP/IP 筛选】选项，单击【属性】按钮，选择【只允许】单选按钮，再单击【添加】按钮，如图 4-23 所示，只填入 80 端口即可。

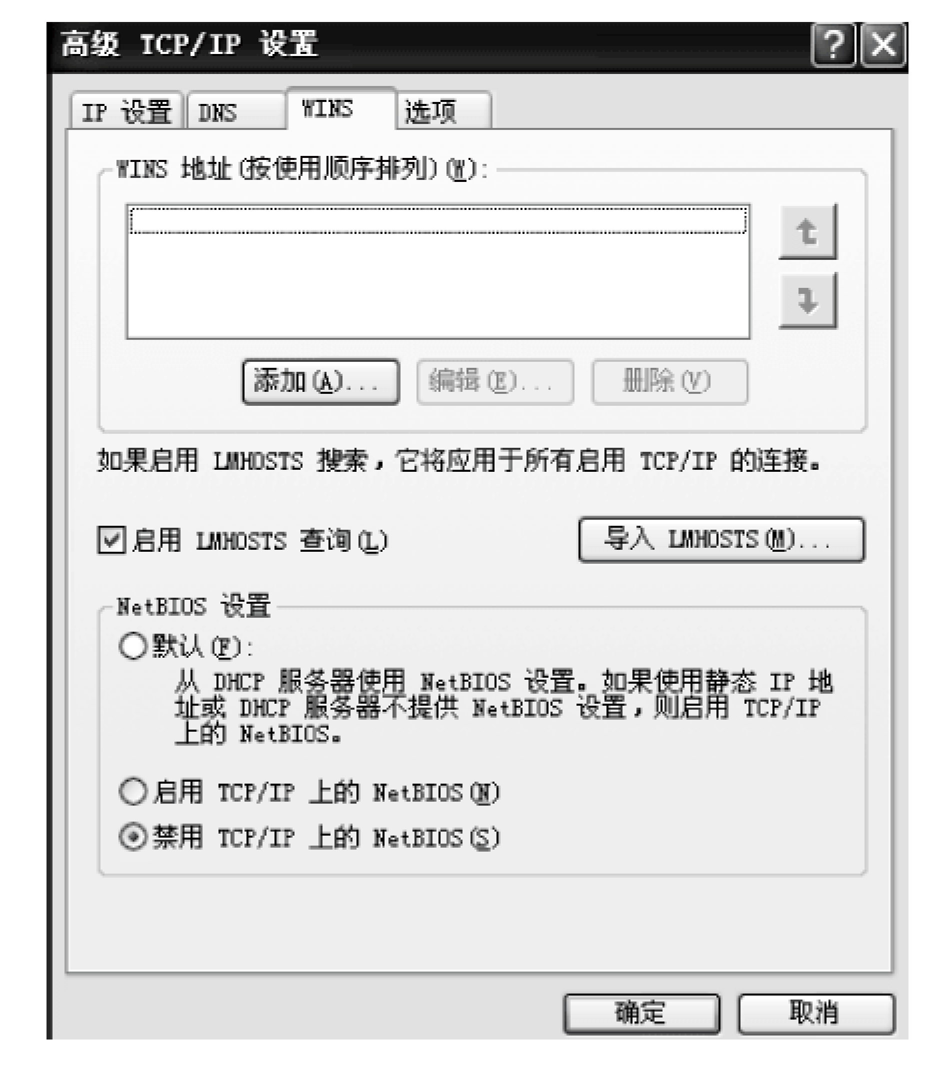


图 4-22　【高级 TCP/IP 设置】对话框



图 4-23　【TCP/IP 筛选】对话框



4.6.2 保证 IIS 自身的安全性

IIS 因其方便性和易用性，成为最受欢迎的 Web 服务器软件之一。但是，它也经常被曝出新的安全漏洞，所以在使用过程中要对 IIS 进行专业的安全配置，使其能提供安全的 Web 服务。

1. IIS 安全安装

在保证系统具有较高安全性的前提下，还要保证 IIS 的安全性。要构建一个安全的 IIS 服务器，在安装时就要充分考虑安全问题。在安装 IIS 时，要注意以下几点：

- 不要将 IIS 安装在系统分区上。默认情况下，IIS 与操作系统安装在同一个分区中，这是一个潜在的安全隐患。因为一旦黑客绕过了 IIS 的安全机制，就有可能入侵到系统分区。如果管理员对系统文件夹的权限设置不是很严谨，入侵者就有可能篡改、删除系统的重要文件，或者利用其他方式进一步获得系统最高权限。将 IIS 安装到其他分区可以避免这个问题。
- 修改 IIS 的默认安装路径。IIS 默认的安装路径是\inetpub，Web 服务的页面路径是\inetpub\wwwroot，这是任何一个熟悉 IIS 的人都知道的，当然黑客也知道。网站的物理路径在入侵过程中起着至关重要的作用，所以一定要更改默认的安装路径来防御这种攻击。
- 打上 Windows 和 IIS 的补丁。只要提高安全意识，经常注意系统和 IIS 的设置情况，并打上最新的补丁，IIS 就会是一个比较安全的服务器平台，能够提供安全稳定的 Web 服务。

2. IIS 的安全配置

(1) 删除不必要的虚拟目录。IIS 安装完成后会在 wwwroot 下生成一些目录，并默认设置了几个虚拟目录，包括 IISHelp、IISAdmin 等，它们的物理路径在系统安装目录下，或在 Program files 目录下，这些虚拟目录没有太大的作用，所以建议将其删掉。

(2) 删除危险的 IIS 组件。在默认安装的 IIS 中，有些组件可能会造成安全威胁，应该将其卸掉，以下是部分黑名单，大家可以根据自己的需要决定是否卸载。

- Internet 服务管理器(HTML)。这是基于 Web 的 IIS 服务器管理页面，一般情况下不应通过 Web 管理服务器，建议卸载。
- SMTP Service 和 NNTP Service。如果不打算使用服务器转发邮件和提供新闻组服务，就可以删除这两项。

(3) 为 IIS 中的文件分类设置权限。除了在操作系统中为 IIS 目录的文件设置必要的权限外，还要在 IIS 管理器中为它们设置权限。通常不要让 IIS 中的文件夹同时拥有写和执行权限，以防止黑客向站点上传并执行恶意代码。另外，目录浏览功能也应禁止，避免暴露站点的目录结构。较好的设置策略是为 Web 站点上不同类型的文件分别建立目录，然后给它们设置合适的权限。例如：

- 静态文件文件夹。包括所有静态文件，如 HTM 或 HTML，给予读权限，拒绝写权限。



- 动态脚本文件夹。包含站点的所有脚本文件，如 cgi、vbs、asp、php、jsp 等，给予执行权限，拒绝读写权限。
- EXE 等可执行程序。包含站点上的二进制执行文件，给予执行权限，拒绝读写权限。
- 图片文件夹。包括站点上的所有图片，应给予读权限，拒绝执行和写权限。
- 上传文件夹。接收各种上传文件，应给予写权限，拒绝执行权限。

（4）删除没用的应用程序映射。IIS 中默认存在很多种应用程序映射，如.htw、.ida、.idq、.asp、.cer、.cdx、.asa、.htr、.idc、.shtm、.shtml、.stm、.php、.jsp 等，通过这些映射，IIS 就能知道什么类型的文件该调用什么类型的动态链接库文件来进行解析。但是在这些映射中，除了.asp、.php、.jsp 这三个程序的映射，其他类型的文件已经很少见了。并且在这些程序映射中，.htr 和.idq/ida 等多个程序映射都被发现存在缓存溢出漏洞，黑客可以利用这些程序映射中存在的缓存溢出获得系统的最高权限。所以需要将这些不需要的程序映射删除。

在【Internet 服务管理器】中，右击网站目录，从弹出的快捷菜单中选择【属性】命令，在打开的【网站目录属性】对话框的【主目录】页面中单击【配置】按钮，打开【应用程序配置】对话框，在【应用程序映射】页面中删除没用的程序映射。

4.6.3　保护日志安全

日志是系统安全策略的一个重要环节，IIS 带有日志功能，能记录所有的用户请求。确保日志的安全能有效提高系统整体安全性。

1. 修改 IIS 日志的存放路径

IIS 日志的默认路径为%WinDir%\System32\LogFiles，这是众所周知的，所以要修改一下其存放路径。在【Internet 服务管理器】中，右击【网站目录】，从弹出的快捷菜单中选择【属性】命令，在打开的【网站目录属性】对话框的【Web 站点】页面中，在选中【启用日志记录】复选框的情况下，单击旁边的【属性】按钮，在【常规属性】页面单击【浏览】按钮或者直接在文本框中输入日志存放路径即可。

2. 修改日志访问权限

日志是为管理员了解系统安全状况而设计的，其他用户没有必要访问，所以最好将日志保存在 NTFS 分区上，设置权限为只有管理员才能访问。

当然，如果条件许可，还可单独设置一个 NTFS 分区用于保存系统日志。这样除了便于管理外，也避免了日志与系统保存在同一分区给系统带来的安全威胁。

4.6.4　防范拒绝服务攻击

DDoS 攻击现在很流行，例如，SYN 使用巨量畸形 TCP 信息包向服务器发出请求，最终导致服务器不能正常工作。可以通过改写注册表信息在一定程度上阻止这类攻击。打开注册



表，将 HKLM\System\CurrentControlSet\Services\Tcpip\Parameters 下的 SynAttackProtect 的值修改为 2。这样当出现 SYN-ATTACK 迹象时，使连接对超时的响应更快。

通过以上的一些安全设置，相信 Web 服务器会安全许多。但是不要认为进行了安全配置的主机就一定安全了。只能说一台主机在某些情况下、一定时间内是安全的，随着网络结构变化、新漏洞的发现、用户操作等，主机的安全状况是实时变化的。只有提高安全意识，注意搜集各种新的漏洞信息、及时升级系统和应用软件，才能做到真正的安全。

4.7 Web 网站的维护和更新

如果网站里的网页文件或者站点的整个目录结构需要更新，就需要网站管理员来对站点进行维护。管理员不可能自己拿着 U 盘跑到机房，把新网页复制到服务器上，通常采用远程的维护方式。常见的有以下几种：

- 将 Web 网站的目录共享，然后设定用户和权限，进行维护。这在局域网里常用。
- 通过远程终端服务，对 Web 网站的内容进行维护。一般主机托管的常用这种方式维护网站。
- 通过远程控制软件，如灰鸽子、PCAnyWhere 等软件远程控制服务器进行站点维护。
- 通过 FTP 服务的方式，设定用户及权限，让用户通过 FTP 方式登录服务器，可以上传文件，维护网站。这是用得最多的一种维护方式。

4.8 上 机 实 战

本节主要练习 Web 站点的建立、配置和发布。

4.8.1 IIS 服务器的安装

IIS 组件可以采用下列步骤安装：

(1) 依次选择【开始】→【程序】→【管理工具】→【管理您的服务器】命令，系统弹出一个服务器管理页面。

(2) 在弹出的页面中选择【添加或删除角色】，选择其中的【应用程序服务器】，单击【下一步】按钮，等待完成安装之后，单击【完成】按钮即可。

4.8.2 配置操作系统的网络和拨号连接

Windows Server 2003 上除网卡对应的 IP 地址外，还可以绑定多个 IP 地址，用于设置多个 Web 和 FTP 站点。Windows Server 2003 对绑定的多个 IP 地址没有限制，而且所有的 IP 地址都可以绑定在同一块网卡上。在服务器上进行 IP 地址的设置及多个 IP 地址绑定的操作步骤如下：

(1) 打开【控制面板】窗口，双击【网络和拨号连接】图标，打开【网络和拨号连接】窗口，



如图 4-24 所示。



图 4-24　【网络和拨号连接】窗口

（2）右击【本地连接】图标，从弹出的快捷菜单中选择【属性】命令，弹出【本地连接 属性】对话框，如图 4-25 所示。

（3）选择【Internet 协议（TCP/IP）】复选框，单击【属性】按钮，弹出【Internet 协议（TCP/IP）属性】对话框，如图 4-26 所示。

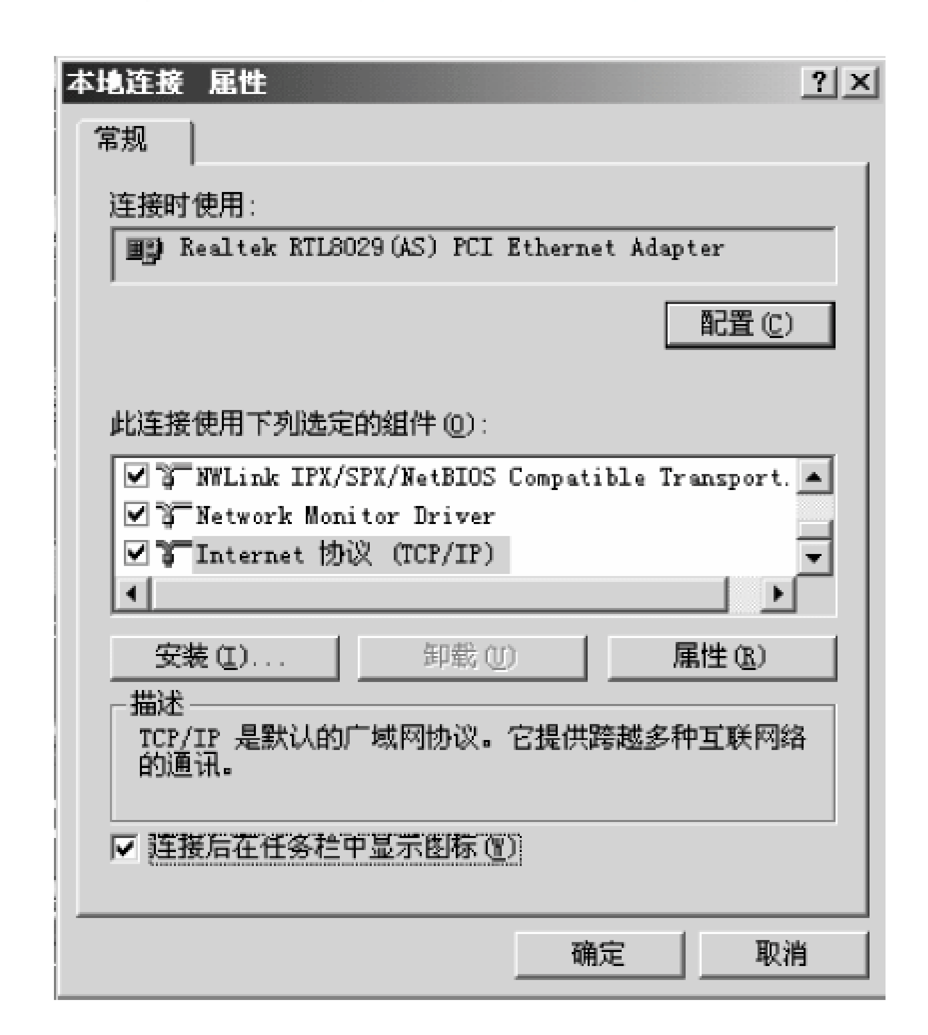


图 4-25　【本地连接 属性】对话框

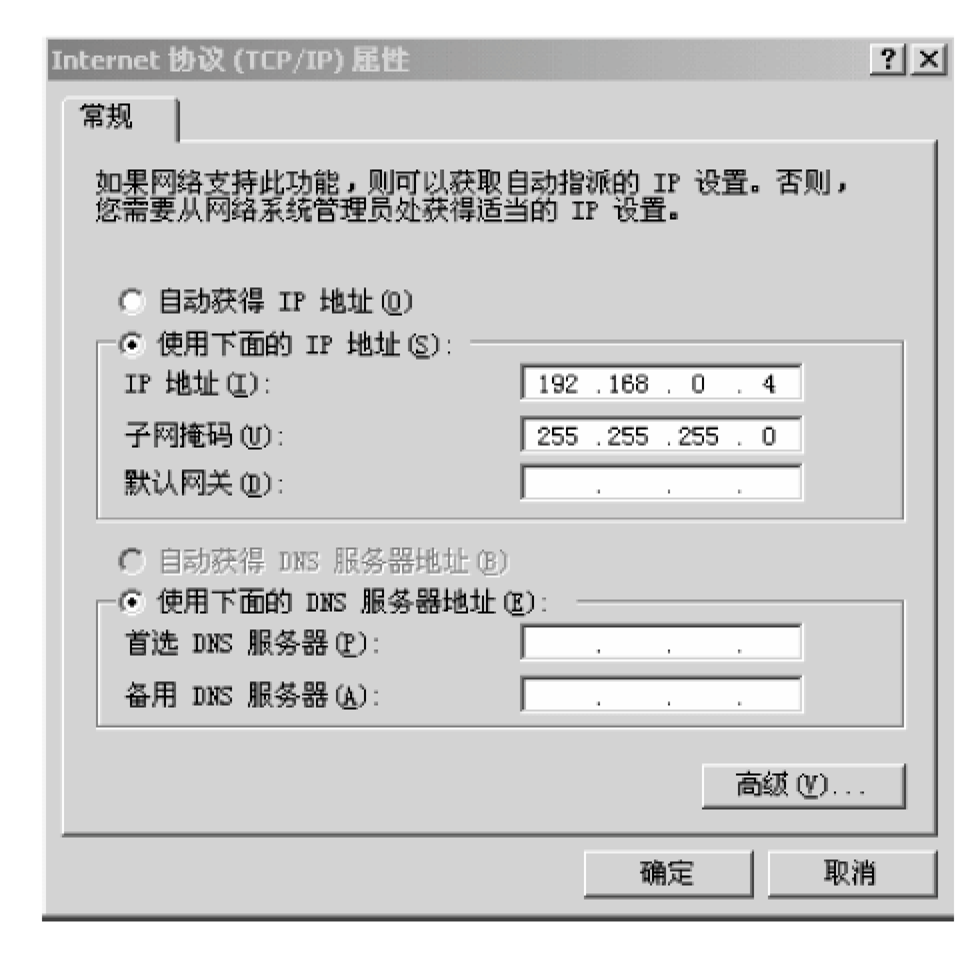


图 4-26　【Internet 协议（TCP/IP）属性】对话框

（4）可以看到，局域网上服务器的 IP 地址为 192.168.0.4，子网掩码为 255.255.255.0。要设置同时绑定在同一网卡上的多个 IP 地址，需要单击【高级】按钮，此时弹出【高级 TCP/IP 设置】对话框，如图 4-27 所示。

（5）单击【添加】按钮，弹出【TCP/IP 地址】对话框，如图 4-28 所示。

（6）在对话框内输入一个 IP 地址和一个相应的子网掩码，单击【添加】按钮，返回【高级 TCP/IP 设置】对话框，输入的 IP 地址及子网掩码显示在对话框的【IP 地址】列表框中。在【高级 TCP/IP 设置】对话框内再次单击【添加】按钮，又弹出【TCP/IP 地址】对话框，再输入一个 IP 地址和一个相应的子网掩码，再单击【添加】按钮，又返回【高级 TCP/IP 设置】对话框，输入的 IP 地址及子网掩码显示在对话框的【IP 地址】列表框中。以此类推，可以输入多个 IP 地址和与之对应的子网掩码。这里新增了两个 IP 地址，即 192.168.0.7 和 192.168.0.8。





图 4-27 【高级 TCP/IP 设置】对话框

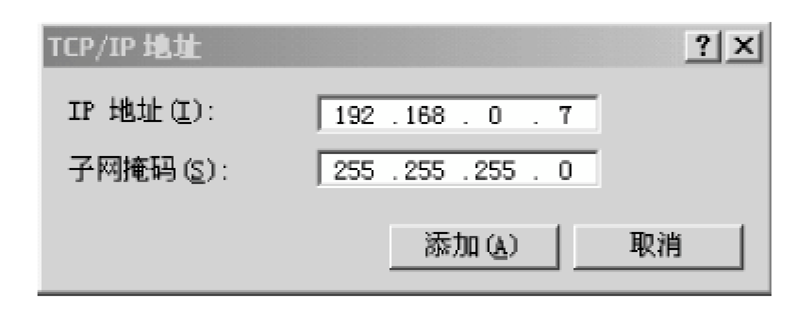


图 4-28 【TCP/IP 地址】对话框

注意：IP 地址可以在 192.168.0.1～192.168.0.254 之间选择，而子网掩码则一律输入 255.255.255.0。

（7）输入完上述两个 IP 地址及其子网掩码后，【高级 TCP/IP 设置】对话框如图 4-29 所示。

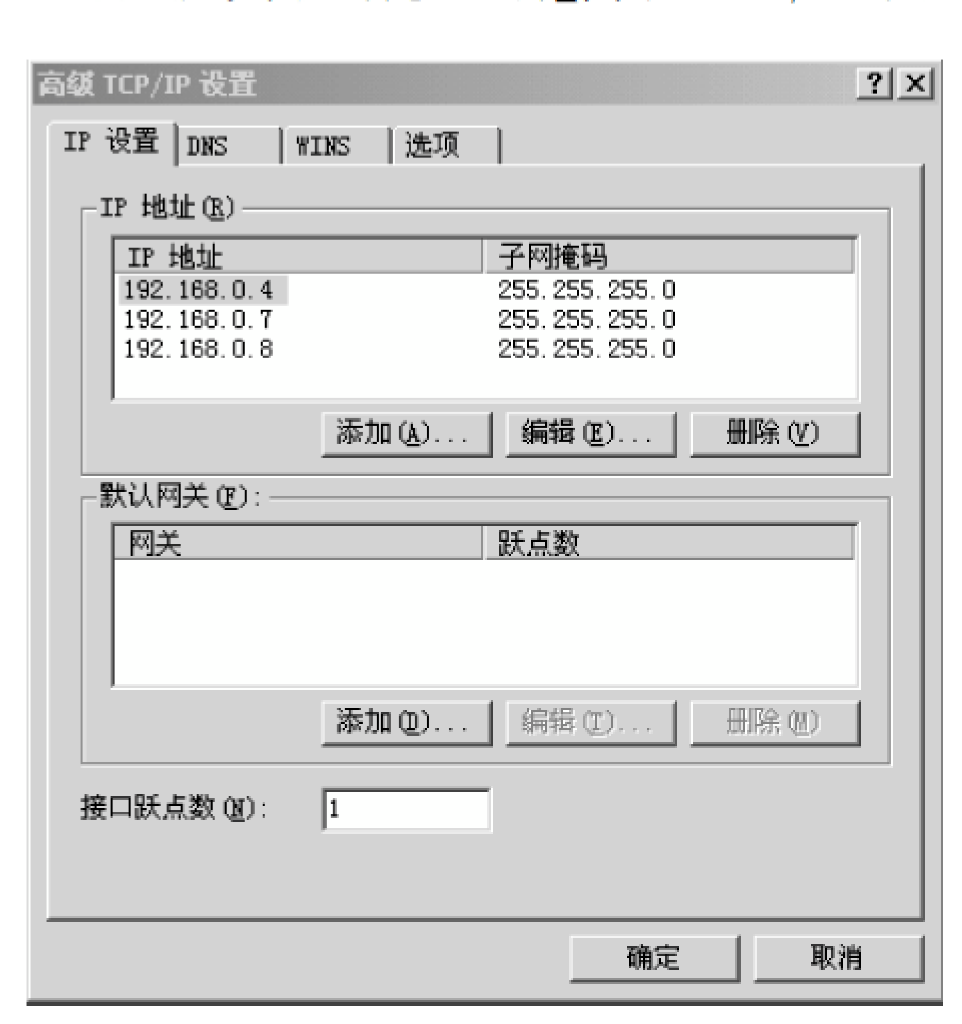


图 4-29 【高级 TCP/IP 设置】对话框

（8）单击【高级 TCP/IP 设置】对话框中的【确定】按钮，返回【Internet 协议（TCP/IP）属性】对话框，单击其中的【确定】按钮，则设置生效，并返回【本地连接 属性】对话框。单击【确定】按钮，关闭此对话框，完成 IP 地址的设置。

4.8.3 Web 站点的建立

在 IIS 中创建一个新的 Web 站点的步骤如下。

（1）依次选择【开始】→【管理工具】→【Internet 信息服务（IIS）管理器】命令，弹出



【Internet 信息服务(IIS)管理器】窗口。

(2) 在【Internet 信息服务(IIS)管理器】窗口的左侧,右击【网站】,从弹出的快捷菜单中选择【新建】→【网站】命令,如图 4-30 所示。



图 4-30 【Internet 信息服务(IIS)管理器】窗口

(3) 接着会弹出【网站创建向导】对话框。利用这个创建向导,可以创建一个新的 Web 站点。

(4) 单击【下一步】按钮,弹出【网站描述】对话框,让用户输入关于新网站的描述信息。

(5) 单击【下一步】按钮,弹出【IP 地址和端口设置】对话框,要求用户输入网站的 IP 地址、网站的 TCP 端口和此网站的主机头,其中网站的 TCP 端口一般使用默认设置,如图 4-31 所示。

(6) 单击【下一步】按钮,弹出【网站主目录】对话框,要求用户输入新建网站内容子目录的根目录在本地磁盘上的路径。

(7) 单击【下一步】按钮,弹出【网站访问权限】对话框。可以在这个对话框中选择网络访问权限,可以允许客户用于读取、写入、浏览、运行脚本等权限,但是一般采用默认设置,如图 4-32 所示。

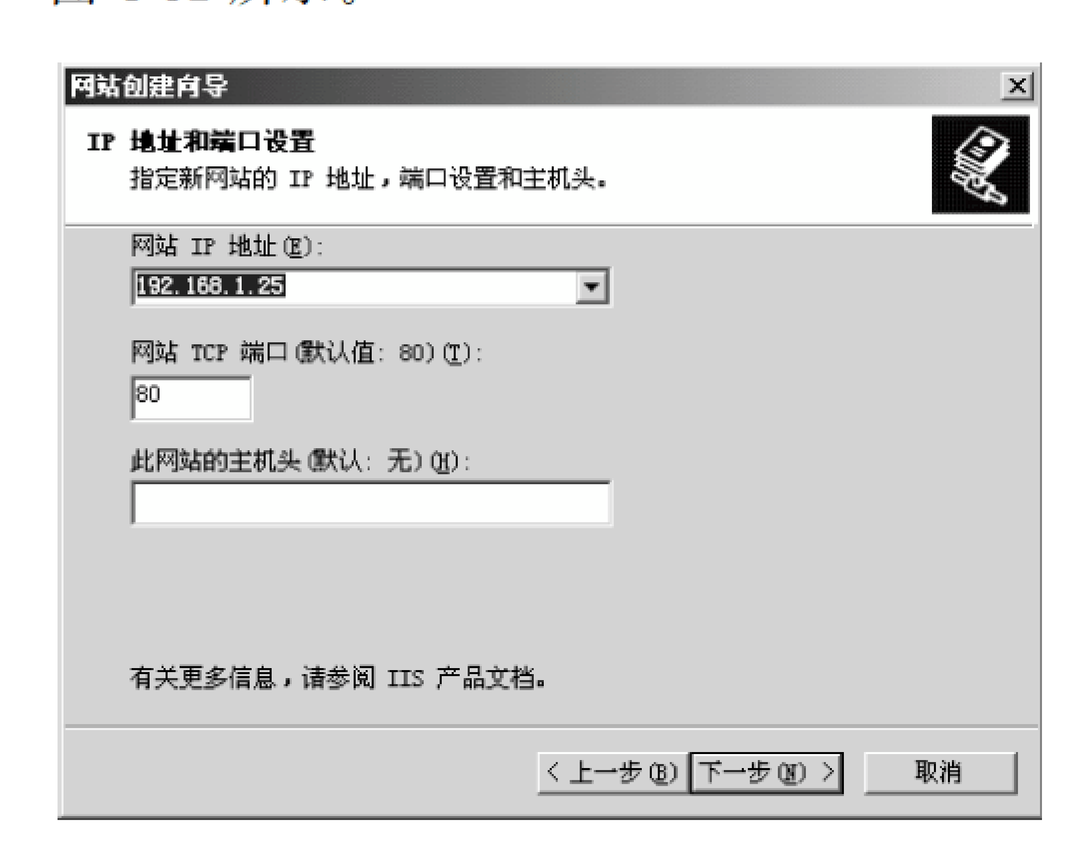


图 4-31 【网站创建向导】对话框

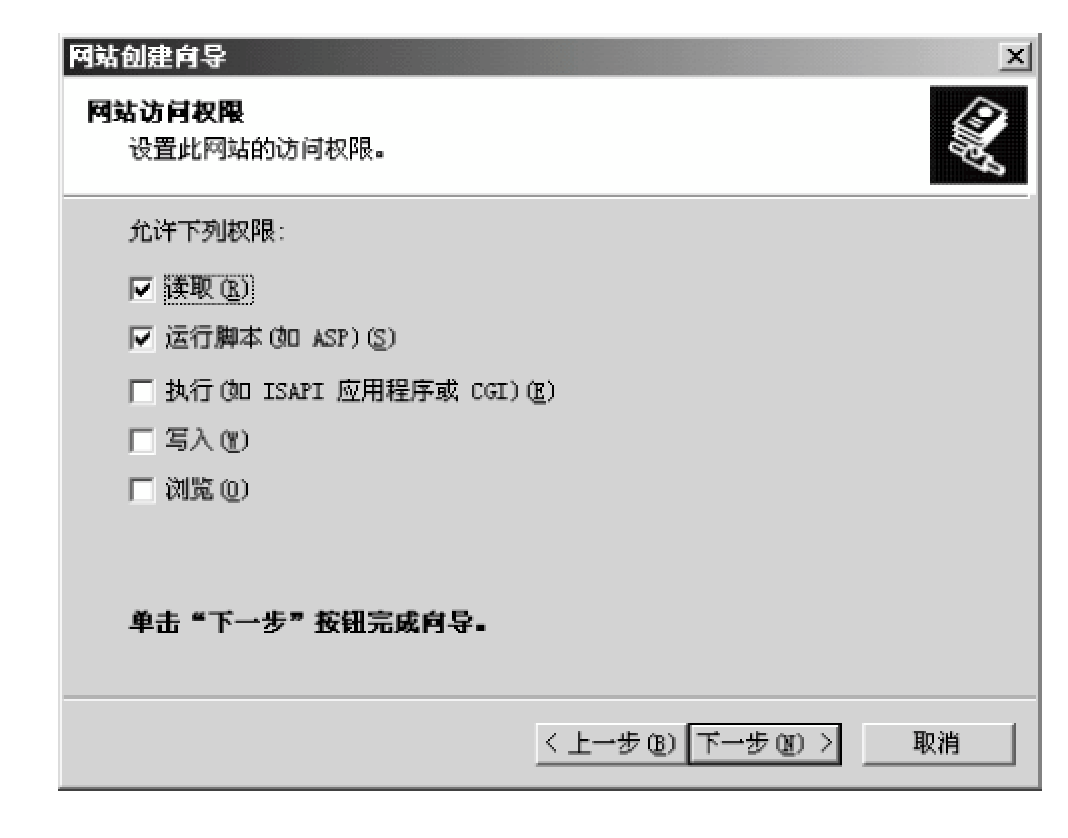


图 4-32 【网站访问权限】对话框

(8) 单击【下一步】按钮,完成新 Web 站点的创建。

4.8.4 Web 站点的管理

在【Internet 信息服务(IIS)管理器】窗口中,右击【需要管理的 Web 站点】,在弹出的快捷菜单中选择【属性】命令,弹出【属性】对话框。在该对话框中按照如下步骤管理 Web 站点:

(1) 在【网站】选项卡中设置站点的 IP 地址和 TCP 端口。

(2) 在【性能】选项卡中可以限制带宽和在相同时间内连接服务器的个数。



(3) 在【主目录】选项卡中可以设置 Web 站点的默认目录,还可以设置访问权限。

(4) 在【文档】选项卡中可以设置或更改默认文档。

4.9 疑难解答

(1) 如何设置服务器直接输入 IP 地址即可访问网站?

由 IIS 6.0 提供 Web 服务时,下面有多个网站,如果想访问 IP 即可访问某个网站,则把需要访问的网站的主机头删除,其他网站设置主机头,这时候再访问服务器的 IP 地址,就可以默认访问到删除了主机头的网站。

(2) 在 Windows Server 2003 中限制日志大小导致 Web 服务停止时如何取消限制?

服务器运行 Windows Server 2003 系统。近来发现只要系统中的某个日志文件达到 512KB,Web 服务将自动停止,只能重新启动系统才能启动 Web 服务。

这种情况很可能是在 IIS 6.0 中限制了日志文件的大小而导致的。可以取消这种限制来解决问题。具体操作方法如下:

① 打开【Internet 信息服务(IIS)管理器】窗口,在左窗格中依次展开【网站】目录。

② 右击 Web 站点名称,从弹出的快捷菜单中选择【属性】命令。

③ 在打开的【Web 站点属性】对话框中切换至【网站】选项卡,然后在【启用日志记录】区域中单击【属性】按钮。

④ 在打开的【日志记录属性】对话框中选中【不限制文件大小】单选按钮,然后连续单击【确定】按钮即可完成设置。

(3) 在 Windows Server 2003 中如何更改"远程桌面连接"的默认端口?

局域网服务器运行 Windows Server 2003 系统。在使用"远程桌面连接"功能时发现,一旦要求远程连接服务器的桌面,其系统自带的防火墙就会自动打开 3389 端口。为了保证服务器系统的安全,要修改"远程桌面连接"的默认端口。

这可以通过更改系统注册表达到上述目的。在注册表中修改该端口的方法为:打开【注册表编辑器】窗口,分别展开 KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp 和 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Te azybPQrminal Server\WinStations\RDP-Tcp 分支,在这两个分支下面均有一个 PortNumber 项,将该项的"十进制"值改为其他数值即可。

(4) 如何为 Web 站点特定文件夹启用日志记录?

一台运行 Windows Server 2003 的局域网服务器,利用其内置的 IIS 6.0 搭建 Web 站点。现在想针对这个网站所对应的目录实施监控,以便观察用户对该站点的访问情况。

这种功能可以采取为网站上的特定文件夹启用日志记录的方法来实现。具体操作方法如下:

① 依次选择【开始】→【所有程序】→【管理工具】→【Internet 信息服务(IIS)管理器】命令,在打开的【Internet 信息服务(IIS)管理器】窗口中依次展开"服务器"和"网站目录"。

② 在展开的目录列表中右击【要设置的 Web 站点】,从弹出的快捷菜单中选择【属性】命令。在打开的【Web 站点属性】对话框中切换至【主目录】选项卡,选中【记录访问】复选框并单击【确定】按钮。



(5) 在 Windows Server 2003 服务器中如何进行 IP 地址和域名限制?

一台基于 Windows Server 2003 系统的服务器,通过 IIS 6.0 自带的 Web 服务组件搭建了 Web 服务器。在服务器上执行 netstat -na 命令查看实时连接时,发现有个 IP 地址发出了大量的 HTTP 连接请求本站 80 端口,可以断定这是一个恶意的连接请求。

这种情况下只需对 IIS 6.0 进行相应的设置即可解决问题。具体操作步骤如下:

① 依次选择【开始】→【程序】→【管理工具】→【Internet 信息服务(IIS)管理器】命令,打开【Internet 信息服务(IIS)管理器】窗口。

② 在左窗格中右击 Web 站点的名称,从弹出的快捷菜单中【属性】命令。打开【站点属性】对话框,然后切换至【目录安全性】选项卡。

③ 单击【IP 地址和域名限制】区域中的【编辑】按钮,打开【IP 地址和域名限制】对话框。默认情况下【授权访问】单选按钮处于选定状态,单击【添加】按钮,打开【拒绝访问】对话框。用户可以选择的拒绝访问类型如下:

- 选中【一台计算机】单选按钮可以拒绝某一台特定计算机访问该站点,只需在【IP 地址】文本框中输入想要拒绝的 IP 地址即可。
- 选中【一组计算机】单选按钮可以限制一组计算机访问该站点,在【网络标识】文本框中输入想限制的子网网段,在【子网掩码】文本框中输入相应的值。如想限制 10.115.223.1～10.115.223.254 这个网段的地址,可以在【网络标识】文本框中输入 10.115.223.0,在【子网掩码】文本框中输入 255.255.255.0 即可。
- 选中【域名】单选按钮可以拒绝来自某一域名的连接请求。在【域名】文本框中输入准备限制的域名即可。设置完毕连续单击【确定】按钮使设置生效。

提示: 拒绝某一个域名连接的设置限制了主域上的各级域名,从而限制了整个域名中所有的主机。这一操作需要 IIS 进行大量的 DNS 反射查询工作,流量比较大,不能轻易使用。

(6) 如何在终端服务器中设置最多连接数?

默认情况下,终端服务器对并发远程连接不限制数量,并且只允许两个并发的管理远程桌面的连接。考虑到节约服务器系统资源问题,用户可以对并发远程连接数量加以限制,以使服务器保持较高的性能。在终端服务器中设置客户端最多连接数的步骤如下:

① 在【RDP-Tcp 属性】对话框中切换到【网卡】选项卡。

② 在【网卡】下拉列表中选中【使用 RDP-Tcp 协议】的网卡。然后选中【最多连接数】单选按钮,并在右侧的微调框中调整并发连接的数值。设置完毕单击【应用】按钮使设置生效。

(7) 如何解决 Windows Server 2003 最大只能上载 200K 的限制?

操作步骤如下:

① 在服务里关闭 iis admin service 服务。

② 找到 windows\\system32\\inesrv\\下的 metabase.xml,打开该文件,找到 ASPMaxRequestEntityAllowed 把它修改为需要的值。

③ 重启 iis admin service 服务。

(8) 如何使用 IIS 6.0 配置静态 Web 网站?

在 Windows Server 2003 系统中成功安装 Web 服务器组件以后,即可使用 IIS 6.0 配置静态 Web 网站。静态网站基于 HTML 语言编写,且不具有交互性。与静态网站相对应



的还有动态网站。在 IIS 6.0 中搭建静态 Web 网站的操作步骤如下：

① 依次选择【开始】→【管理工具】→【Internet 信息服务(IIS)管理器】命令，打开【Internet 信息服务(IIS)管理器】窗口。在左窗格中展开【网站】目录，右击【默认网站】选项，在弹出的快捷菜单中选择【属性】命令。

② 打开【默认网站 属性】对话框，选择【网站】选项卡，单击【IP 地址】右侧的下拉三角按钮，并选中该站点要绑定的 IP 地址。

③ 选择【主目录】选项卡，单击【本地路径】文本框右侧的【浏览】按钮，选择网站程序所在的主目录并单击【确定】按钮。

④ 选择【文档】选项卡，选中【启用默认内容文档】复选框。然后在文档列表中查找是否有网站首页文件的名称(静态网站首页文件名称一般为 index.htm)。如果没有，则单击【添加】按钮，在打开的【添加内容页】对话框中输入网站首页文件名(如 index.html)，并单击【确定】按钮。

⑤ 返回【默认网站 属性】对话框，并单击【确定】按钮。至此，静态网站搭建完毕，用户只要将开发的网站源程序复制到所设置的网站主目录中，即可使用指定的 IP 地址访问该网站。

(9) 如何在 IIS 6.0 中使用命令行脚本管理网站和 Web 虚拟目录?

IIS 6.0 包含多个受支持的命令行脚本，这些脚本可使用 Windows Management Instrumentation (WMI) 提供程序在运行 IIS 的本地或远程计算机上配置和管理 IIS 元数据库配置。可以使用这些脚本自动执行任务、远程管理站点和资源并利用批处理文件创建和管理对象。Microsoft 支持 IIS 中包含的命令行脚本，如果要修改受支持的脚本，请使用新的文件名保存它，以使原始脚本保持不变。

这些脚本位于 %SystemRoot\System32 文件夹中。要运行脚本和可执行文件，必须是本地计算机上的管理员组成员。要打开【命令提示符】窗口以执行本文所介绍的任何任务，请按照下列步骤操作：

① 依次选择【开始】→【运行】命令，调出【运行】对话框，如图 4-33 所示。在【打开】文本框中输入 cmd，然后单击【确定】按钮，调出【命令提示符】窗口，如图 4-34 所示。

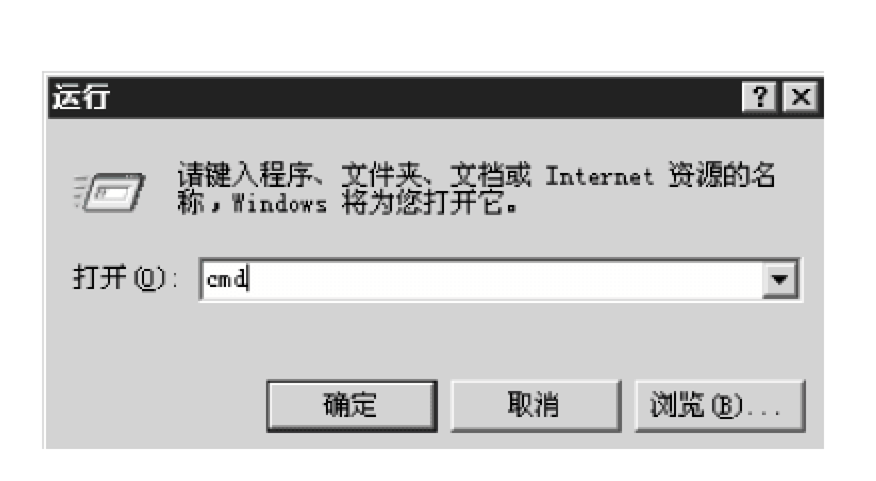


图 4-33 【运行】对话框



图 4-34 【命令提示符】窗口

② 在提示符后输入以下代码，然后按 Enter 键：

```
cd %systemroot%\system32
```





在 IIS 6.0 中，可以使用 iisweb.vbs 脚本创建和管理网站，方法如下所述：

① 创建新网站。要创建一个新的网站配置，请使用 iisweb /create 命令。此命令不会创建内容，但它会设置文件夹结构和一些 IIS 配置文件。在使用 iisweb.vbs 创建新的网站时，只需指定创建站点所需的基本属性，并确定其内容即可。

iisweb /create 命令的语法格式如下：

```
iisweb /create PathSiteName [/b Port] [/i IPAddress] DisplayName [/d HostHeader] [/dontstart]
[/s Computer [/u [Domain\]User /p Password]]
```

iisweb /create 使用的参数详解如下。

- Path：指定在本地计算机上网站内容文件的位置。如果指定的路径不存在，iisweb 将创建它。
- SiteName：必选参数，指定网站名称。
- /b Port：指定网站的 TCP 端口号。默认端口为 80。
- /i IPAddress：指定网站的 IP 地址。默认设置为全部未分配，此设置将计算机上所有未分配给其他站点的 IP 地址都分配给该站点。
- /d HostHeader：指定网站的主机头名称。默认情况下，站点没有主机头名称，必须根据其 IP 地址或端口号才能识别该站点。
- /dontstart：此参数指定网站在创建后不会自动启动。
- /s Computer：在指定的远程计算机上运行脚本。输入不带反斜线的计算机名或 IP 地址。
- /u [Domain\]User：使用指定用户账户的权限来运行脚本。此账户必须是远程计算机上的管理员组成员。默认情况下，使用本地计算机当前用户的权限来运行脚本。
- /p Password：指定在 /u 参数中指定的用户账户的密码。

以下命令行可在本地计算机上创建一个名为 My Site 的网站配置。源文件位于 C:\MySource 文件夹中，并指定了主机头名称：

```
iisweb /create C:\MySource "My Site" /d www.mywebsite.com /dontstart
```

② 删除网站。要删除网站配置，请使用 iisweb /delete 命令。如果计划将站点移到一个新的统一资源定位器或服务器上，或者希望将其完全删除，则此命令很有用。在使用此命令后，站点的内容不会受到影响，但用户不能再访问该站点。

iisweb /delete 命令的语法格式如下：

```
iisweb /delete WebSite [WebSite...][/s Computer [/u [Domain\]User/p Password]]
```

iisweb /delete 命令使用的参数详解如下。

- WebSite：必选参数，指定网站的唯一描述性名称或元数据库路径。如果多个网站使用同一描述性名称，则必须使用元数据库路径才能识别网站。
- /s Computer：在指定的远程计算机上运行脚本。输入不带反斜线的计算机名或 IP 地址。
- /u [Domain\]User：使用指定用户账户的权限来运行脚本。此账户必须是远程计



算机上的管理员组成员。默认情况下，使用本地计算机当前用户的权限来运行脚本。

- /p Password：指定在 /u 参数中指定的用户账户的密码。

以下命令行可在本地计算机上删除一个名为 My Site 的网站配置：

```
iisweb /delete "My Site"
```

③ 查询网站。要查询或列出网站，请使用 iisweb /query 命令。如果要在本地计算机或远程计算机上检查网站的状态或属性，则此命令很有用。

iisweb /query 命令的语法格式如下：

```
iisweb /query WebSite [WebSite...][/s Computer [/u [Domain\]User /p Password]]
```

iisweb /query 命令使用的参数详解如下。

- WebSite：限制对指定网站的查询。使用网站的唯一描述性名称或元数据库路径。如果忽略此参数，则会显示计算机上的所有网站。
- /s Computer：在指定的远程计算机上运行脚本。输入不带反斜线的计算机名或 IP 地址。
- /u [Domain\]User：使用指定用户账户的权限来运行脚本。此账户必须是远程计算机上的管理员组成员。默认情况下，使用本地计算机当前用户的权限来运行脚本。
- /p Password：指定在 /u 参数中指定的用户账户的密码。

以下命令行可在本地计算机上显示网站：

```
iisweb /query
```

在 IIS 6.0 中，可以使用 iisvdir.vbs 脚本创建和管理 Web 虚拟目录，方法如下所述：

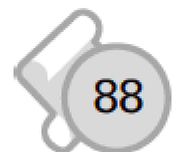
① 创建新的 Web 虚拟目录。要创建一个新的 Web 虚拟目录，请使用 iisvdir /create 命令。此命令不会创建内容，但它会设置虚拟目录结构和 IIS 配置文件。在使用 iisvdir.vbs 创建一个新的 Web 虚拟目录时，只需指定创建站点所需的基本属性，并确定其内容。

iisvdir /create 命令的语法格式如下：

```
iisvdir /create WebSite [/Virtual Path]Name Physical Path [/s Computer [/u [Domain\] User /p
Password]]
```

iisvdir /create 命令使用的参数详解如下。

- WebSite：必选参数，指定网站的唯一描述性名称或元数据库路径。
- Virtual Path：指定网站中虚拟目录的路径。如果虚拟目录不在网站的根目录处，则此参数是必需的。
- Name：必选参数，指定虚拟目录的名称。虚拟目录的名称不必是唯一的。
- Physical Path：指定在本地计算机上虚拟目录内容所在的物理文件夹。如果指定的文件夹不存在，iisvdir 会创建它。
- /s Computer：在指定的远程计算机上运行脚本。输入不带反斜线的计算机名或 IP 地址。



- /u [Domain\]User：使用指定用户账户的权限来运行脚本。此账户必须是远程计算机上的管理员组成员。默认情况下，使用本地计算机当前用户的权限来运行脚本。
- /p Password：指定在 /u 参数中指定的用户账户的密码。

以下命令行可在本地计算机上 test 网站的根目录处创建 down 虚拟目录，并将该目录与在 D:\download\web 文件夹中当前存储的内容相关联：

```
iisvdir /create test down d:\download\web
```

② 删除 Web 虚拟目录。要删除 Web 虚拟目录，请使用 iisvdir /delete 命令。

iisvdir /delete 命令语法格式如下：

```
iisvdir /delete WebSite [/Virtual Path]Name [/s Computer [/u [Domain\]User /p Password]]
```

iisvdir /delete 命令使用的参数详解如下。

- WebSite：必选参数，指定网站的唯一描述性名称或元数据库路径。
- Virtual Path：指定网站中虚拟目录的路径。如果虚拟目录不在网站的根目录处，则此参数是必需的。
- Name：必选参数，指定虚拟目录的名称。虚拟目录的名称不必是唯一的。
- /s Computer：在指定的远程计算机上运行脚本。输入不带反斜线的计算机名或 IP 地址。
- /u [Domain\]User：使用指定用户账户的权限来运行脚本。此账户必须是远程计算机上的管理员组成员。默认情况下，使用本地计算机当前用户的权限来运行脚本。
- /p Password：指定在 /u 参数中指定的用户账户的密码。

以下命令行可从本地计算机上的 test 网站中删除 down 虚拟目录。注意，down 虚拟目录的所有虚拟子目录也将被删除。

```
iisvdir /delete test/down
```

习　题

1. 填空题

(1) 在互联网中，WWW 服务器与 WWW 浏览器之间的信息传递使用________协议。

(2) URL 一般由三部分组成，它们是________、________和________。

(3) WWW 服务通过 HTML 和________两种技术为基础，为用户提供界面一致的信息浏览系统，实现各种信息的链接。

2. 选择题

(1) 在 WWW 服务器服务系统中，编制的 Web 页面应符合(　)。

A. HTML 规范　　B. RFC822 规范　　C. MIME 规范　　D. HTTP 规范

(2) 下面选项中表示超文本传输协议的是(　)。

A. RIP　　B. HTML　　C. HTTP　　D. ARP

(3) 在 Internet 上浏览时，浏览器和 WWW 服务器之间传输网页使用的协议是(　　)。

A. SMTP　　B. HTTP　　C. FTP　　D. Telnet



(4) 在 Windows 系统中下列 URL 的表达方式是错误的是(　　)。

A. http://www.sise.com.cn

B. ftp://172.16.3.250

C. rtsp://172.16.102.101/hero/01.rm

D. http:/www.sina.com.cn

(5) 超文本 HTML 是指(　　)。

A. 包含有许多文件的文本　　B. Internet 上传输的文本

C. 包含有多种媒体的文本　　D. 包含有链接关系的文本

3. 思考题

(1) 如何发布已经制作好的网站?

(2) 如何建立虚拟主机?

第5章　FTP服务器的配置与应用

本章要点

- 了解常用的 FTP 命令
- 掌握用 IIS 建立 FTP 站点的方法
- 掌握用 Serv-U 建立 FTP 服务器的方法
- 了解 FTP 服务器的安全设置方法

文件传输协议(File Transfer Protocol,FTP)是一个用于简化 IP 网络上系统之间文件传送的协议。采用 FTP 协议可使用户高效地从 Internet 上的 FTP 服务器下载大量的数据文件,以达到资源共享和传递信息的目的。目前,FTP 服务在网络服务中起着十分重要的作用,得到了广泛应用。

5.1　了解 FTP 服务

在网络上常常需要将一台计算机上的文件复制到另一台计算机上,这就是文件传输服务。文件传输协议(FTP)是用于在 TCP/IP 网络上两台计算机间进行文件传输的协议,其位于 TCP/IP 协议堆栈的应用层,也是最早用于因特网上的协议之一。FTP 允许在两个异构体系之间进行 ASCII 码或 EBCDIC 码(扩充的二进制码十进制转换)字符集的传输,这里的异构体系是指采用不同操作系统的两台计算机。

与大多数的因特网服务一样,FTP 使用客户机—服务器模式,即由一台计算机作为 FTP 服务器提供文件传输服务,而由另一台计算机作为 FTP 客户端提出文件服务请求并得到授权的服务。FTP 服务器与客户机之间使用 TCP 作为实现数据通信与交换的协议。然而与其他客户/服务器模型不同的是,FTP 客户与服务器之间建立的是双重连接,一个是控制连接(Control Connection);另一个是数据传送连接(Data Transfer Connection)。控制连接传送命令,告诉服务器将传送哪个文件。数据传送连接也使用 TCP 作为传输协议,传送所有数据。

在 FTP 的服务器上,只要启动了 FTP 服务,则总是有一个 FTP 的守护进程在后台运行以随时准备对客户端的请求做出响应。当客户端需要文件传输服务时,其将首先设法打开一个与 FTP 服务器之间的控制连接,在连接建立过程中服务器会要求客户端提供合法的登录名和密码。在许多情况下,使用匿名登录,即采用 anonymous 为用户名,自己的 E-mail



地址作为密码。一旦该连接被允许建立,其相当于在客户机与 FTP 服务器之间打开了一个命令传输的通信连接,所有与文件管理有关的命令将通过该连接被发送至服务器端执行。该连接在服务器端使用 TCP 端口号的默认值为 21,并且该连接在整个 FTP 会话期间一直存在。每当请求文件传输即要求从服务器复制文件到客户机时,服务器将再形成另一个独立的通信连接,该连接与控制连接使用不同的协议端口号。默认情况下,在服务器端使用 20 号 TCP 端口,所有文件可以以 ASCII 模式或二进制模式通过该数据通道传输。一旦客户请求的一次文件传输完毕则该连接就要被拆除,新一次的文件传输需要重新建立一条数据连接。但前面所建立的控制连接则被保留,直至全部的文件传输完毕客户端请求退出时才会被关闭。

用户可以使用 FTP 命令来进行文件传输,这称为交互模式。当用户交互使用 FTP 时,FTP 发出一个提示,用户输入一条命令,FTP 执行该命令并发出下一提示。FTP 允许文件沿任意方向传输,即文件可以上传与下载。在交互方式下,也提供了相应的文件上传与下载的命令。前面介绍过,FTP 有文本方式与二进制方式两种文件传输类型,所以在进行文件传输之前,还要选择相应的传输类型:根据远程计算机文本文件所使用的字符集是 ASCII 或 EBCDIC,用户可以用 ASCII 或 EBCDIC 命令来指定文本方式传输;所有非文本文件,例如,声音剪辑或者图像等都必须用二进制方式传输,用户输入 binary 命令可将 FTP 设置成二进制模式。如在 Windows 2000 操作系统下可使用如下形式的 FTP 命令:

```
FTP [-d-g-i-n-t-v] [host]
```

其中,host 代表主机名或者主机对应的 IP 地址;d 表示允许调试;g 表示不允许在文件名中出现“*”和“?”等通配符;i 表示多文件传输时,不显示交互信息;n 表示不利用 $HOME/netrc 文件进行自动登录;t 表示允许分组跟踪;v 表示显示所有从远程服务器上返回的信息;“[]”表示其中的内容为命令的可选参数。

用户输入 FTP 命令如 ftp 10.50.8.3 后,屏幕就会显示“FTP >”提示符,表示用户进入 FTP 的工作模式。在该模式下用户可输入 FTP 操作的子命令。常用的 FTP 子命令及其功能如表 5-1 所示。

表 5-1　常用 FTP 子命令及其功能

命令名称	对应的功能
ASCII	进入 ASCII 方式,传送文本文件
BINARY	传送二进制文件;进入二进制方式
BYE 或 QUIT	结束本次文件传输,退出 FTP 程序
CD dir	改变远程当前目录
LCD dir	改变本地当前目录
DIR 或 LS [remote-dir] [local-file]	列表远程目录
GET remote-file [local-file]	获取远程文件
MGET remote-files	获取多个远程文件,可以使用通配符
PUT local-file [remote-file]	将一个本地文件传送到远程主机上
MPUT local-files	将多个本地文件传送到远程主机上,可以使用通配符
DELETE remote-file	删除远程文件
MDELETE remote-files	删除多个远程文件

续表

命 令 名 称	对应的功能
MKDIR dir-name	在远程主机上创建目录
RMDIR dir-name	删除远程目录
OPEN host	与指定主机的 FTP 服务器建立连接
CLOSE	关闭与远程 FTP 程序的连接
PWD	显示远程当前目录
STATUS	显示 FTP 程序的状态
USER user-name [password] [account]	向 FTP 服务器表示用户身份

5.2　安装、测试 FTP 站点

5.2.1　安装 FTP 站点

安装 FTP 站点的操作步骤如下：

(1) 依次选择【开始】→【控制面板】→【添加/删除程序】→【添加/删除 Windows 组件】命令，打开如图 5-1 所示的【Windows 组件向导】对话框。在【组件】列表框中选择【应用程序服务器】复选框。

(2) 单击【详细信息】按钮，打开如图 5-2 所示的【应用程序服务器】对话框，选中【Internet 信息服务(IIS)】复选框。

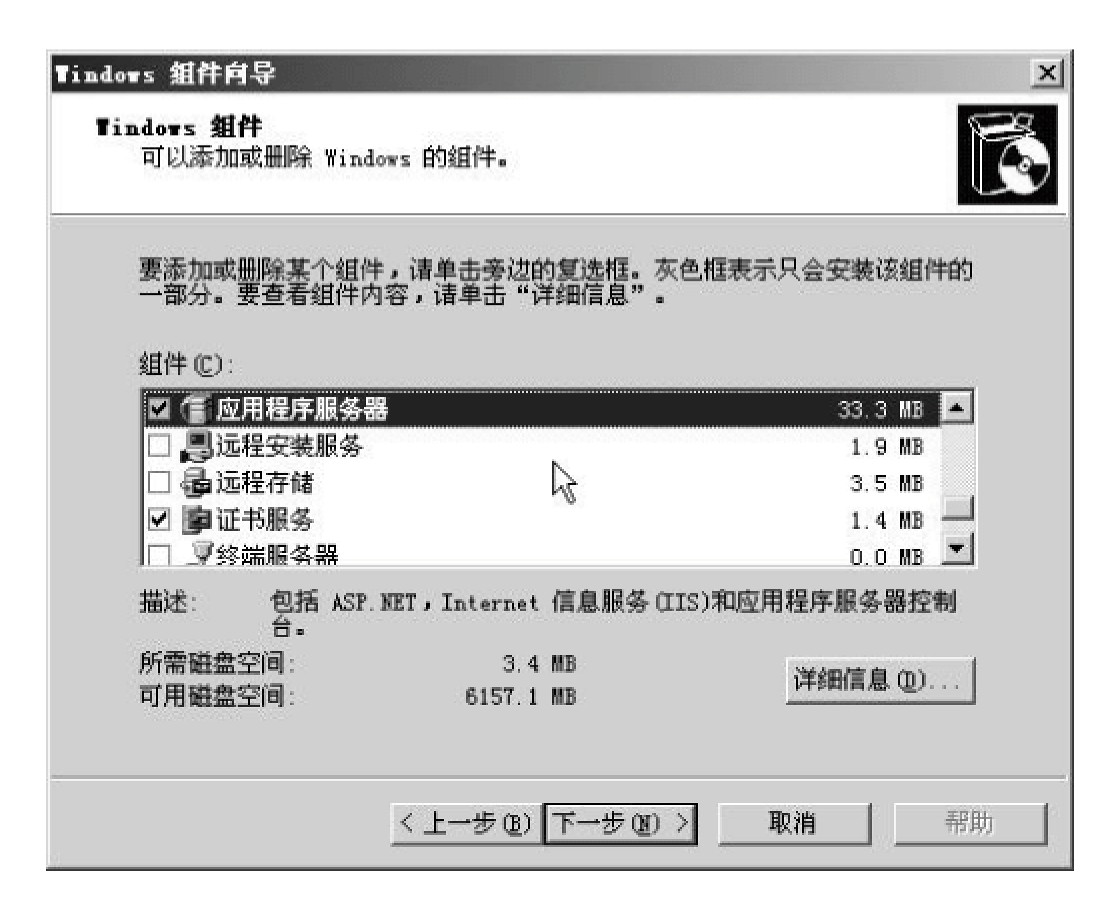


图 5-1　【Windows 组件向导】对话框

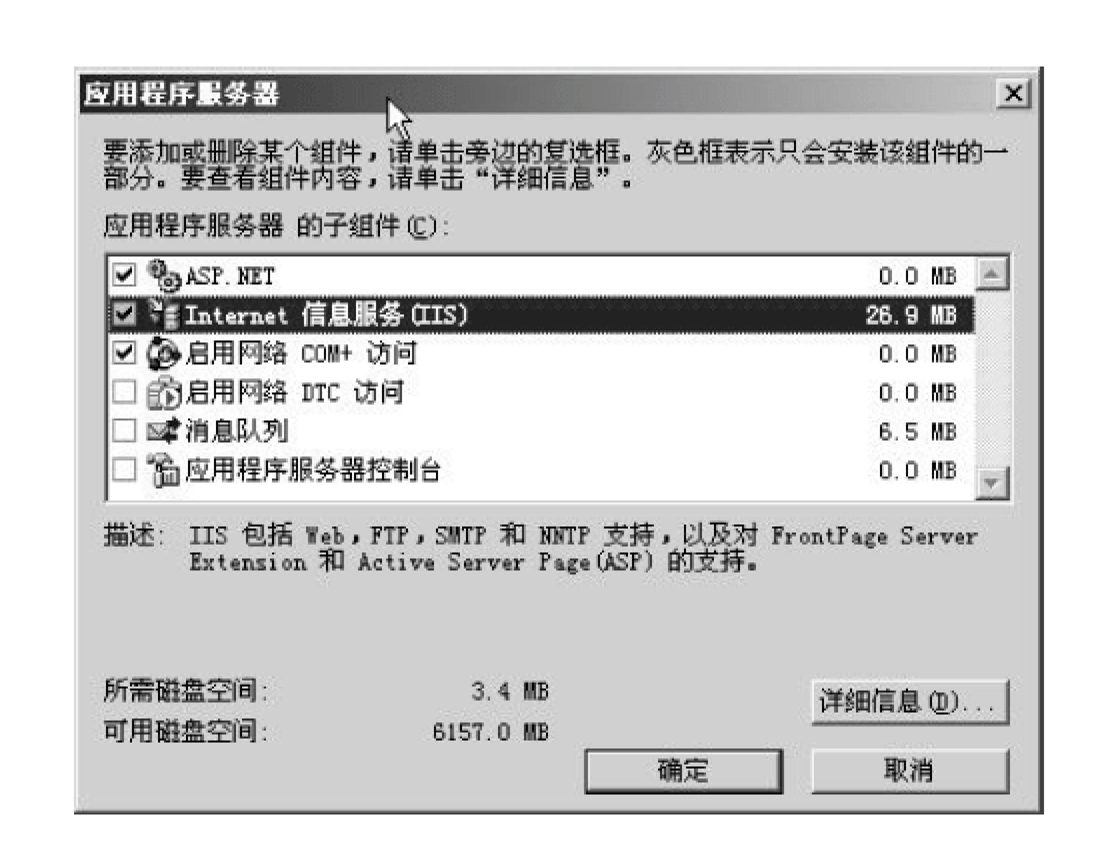


图 5-2　【应用程序服务器】对话框

(3) 单击【确定】按钮，开始安装 FTP 组件。

5.2.2　测试已安装的 FTP 站点

通过以上方法安装好 FTP 组件后，还需要对 FTP 站点进行测试，以确保 FTP 服务已经正常运行。具体方法如下。



（1）依次选择【开始】→【管理工具】→【Internet 信息服务(IIS)管理器】命令，打开如图 5-3 所示的【Internet 信息服务(IIS)管理器】窗口。



图 5-3 【Internet 信息服务(IIS)管理器】窗口

（2）查看是否有一个“默认 FTP 站点”。如果看不到这个默认站点，就表示 FTP 组件安装失败，需按 5.2.1 小节所述办法重新安装一遍或者检查一下 Windows Server 2003 的系统安装盘是否有问题。

5.3 建立 FTP 站点

一般而言，建立 FTP 站点有两大类方法。一种是利用 IIS 中的 FTP 组件；另一种就是利用 Serv-U、EFTP 等第三方 FTP 服务器软件。第一种方法普遍应用在虚拟主机中，但提供的功能比较单一；第二种方法由于操作方便、功能强大，应用非常广泛，但要经过专业的安全设置才能投入使用，否则会给服务器带来安全隐患。两种方法各有优缺点。下面首先介绍用 IIS 建立 FTP 站点的方法。利用第三方软件建立 FTP 站点的方法在 5.6 节中介绍。

5.3.1 利用“默认 FTP 站点”建立 FTP 站点

在安装了 FTP 组件后，系统会自动创建一个“默认 FTP 站点”。“默认 FTP 站点”的特点为：

- 使用系统默认的 21 号 TCP 端口。
- “默认 FTP 站点”的主目录为 C:\inetpub\ftproot，其中“C:”为 Windows Server 2003 的安装分区。
- 适用于所有的 IP 地址。如果该 FTP 服务器上同时存在多个 IP 地址，通过每一个 IP 地址都可以访问到“默认 FTP 站点”。

5.3.2 利用其他主目录建立 FTP 站点

利用“默认 FTP 站点”建立 FTP 站点，虽然操作方便，但却存在一些问题。例如，由于“默认 FTP 站点”与 Windows Server 2003 位于同一个硬盘分区，所以 FTP 站点的内容在安全性和空间上都受到了限制。另外，由于“默认 FTP 站点”的许多设置都是系统默认的，主要用于在安装 FTP 组件后对 FTP 服务进行测试，所以“默认 FTP 站点”的功能也很有限。





因此，对于一些较大型的、在 Internet 上发布的 FTP 站点，一般不使用"默认 FTP 站点"，而是利用其他主目录来建立 FTP 站点。

5.3.3 建立虚拟目录 FTP 站点

将 FTP 站点的主目录称为实际目录或物理目录，例如前面介绍的"默认 FTP 站点"对应的主目录 C:\inetpub\ftproot。以实际目录发布的 FTP 站点为依托，可以将位于本地计算机或网络中其他计算机上的物理目录发布为 FTP 站点，这种站点对应的目录叫做虚拟目录。每个虚拟目录都有一个别名，通过在主 FTP 站点的名称后加上"/虚拟目录别名"就可以访问到该虚拟目录站点。操作步骤如下：

(1) 右击图 5-3 所示的"默认 FTP 站点"，在弹出的快捷菜单中依次选择【新建】→【虚拟目录】命令，调出【虚拟目录创建向导】对话框，如图 5-4 所示。

(2) 单击【下一步】按钮，设置虚拟目录的路径，如图 5-5 所示。

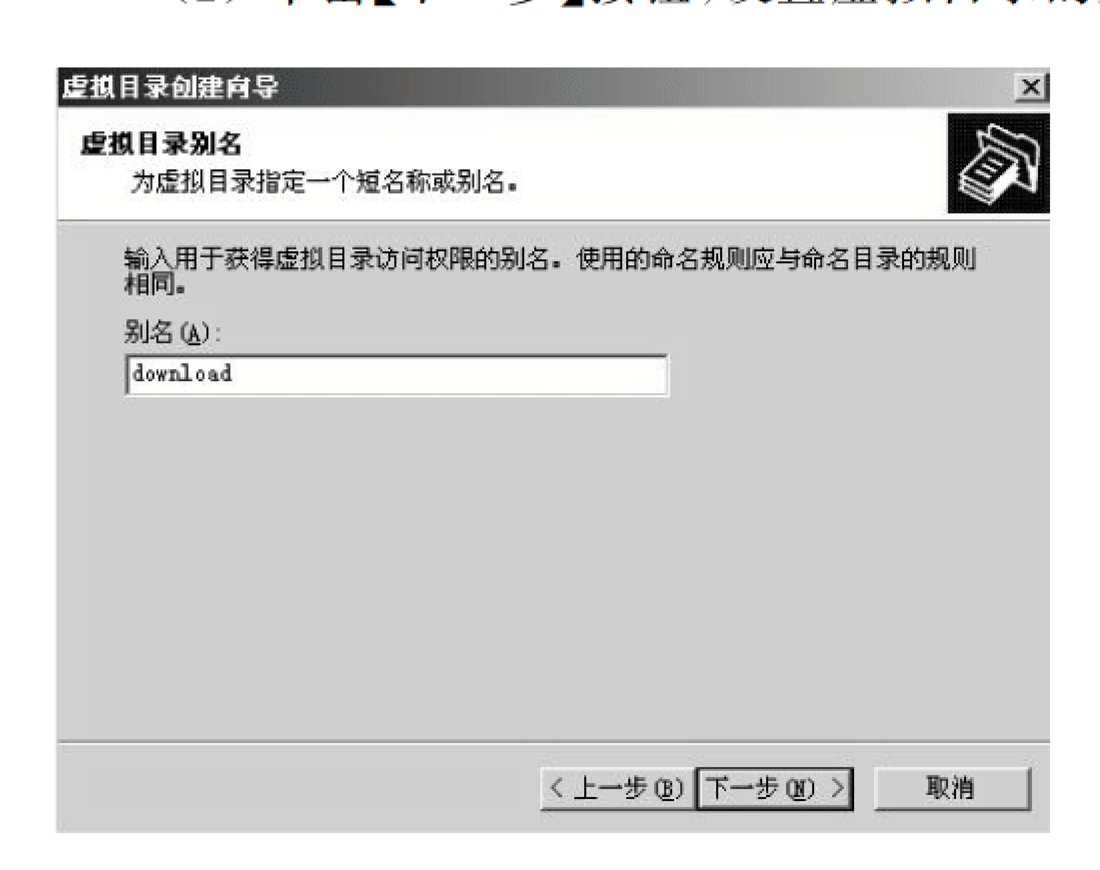


图 5-4 【虚拟目录创建向导】对话框—设置别名

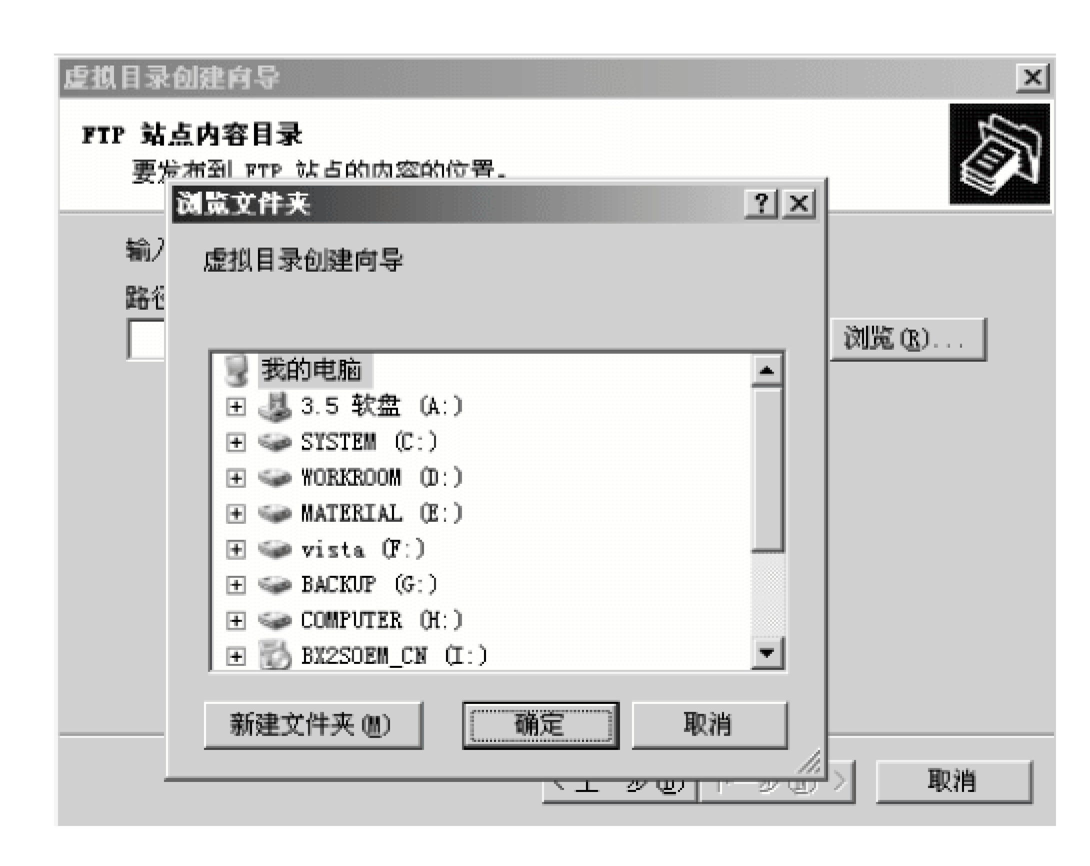


图 5-5 【虚拟目录创建向导】对话框—选择路径

(3) 单击【下一步】按钮，设置虚拟目录的权限。这样就完成了虚拟目录的设置。用户访问时，只需在站点后加上/download 就可以访问到该虚拟目录站点。

5.3.4 创建具有特殊要求的 FTP 站点

Windows Server 2003 的 IIS 提供了 FTP 用户隔离功能，它可以让每个用户在同一台 FTP 服务器上分别拥有一个专用的文件夹。这样，当不同的用户登录 FTP 站点时，系统会根据不同的用户访问不同的文件夹。

创建具有特殊要求的 FTP 站点的操作步骤如下：

(1) 右击图 5-3 所示的"默认 FTP 站点"，在弹出的快捷菜单中依次选择【新建】→【FTP 站点】命令，调出【FTP 站点创建向导】对话框，如图 5-6 所示。

(2) 在【描述】文本框中输入站点描述后，单击【下一步】按钮，调出图 5-7 所示的对话框。从中设置 FTP 用户隔离类型。



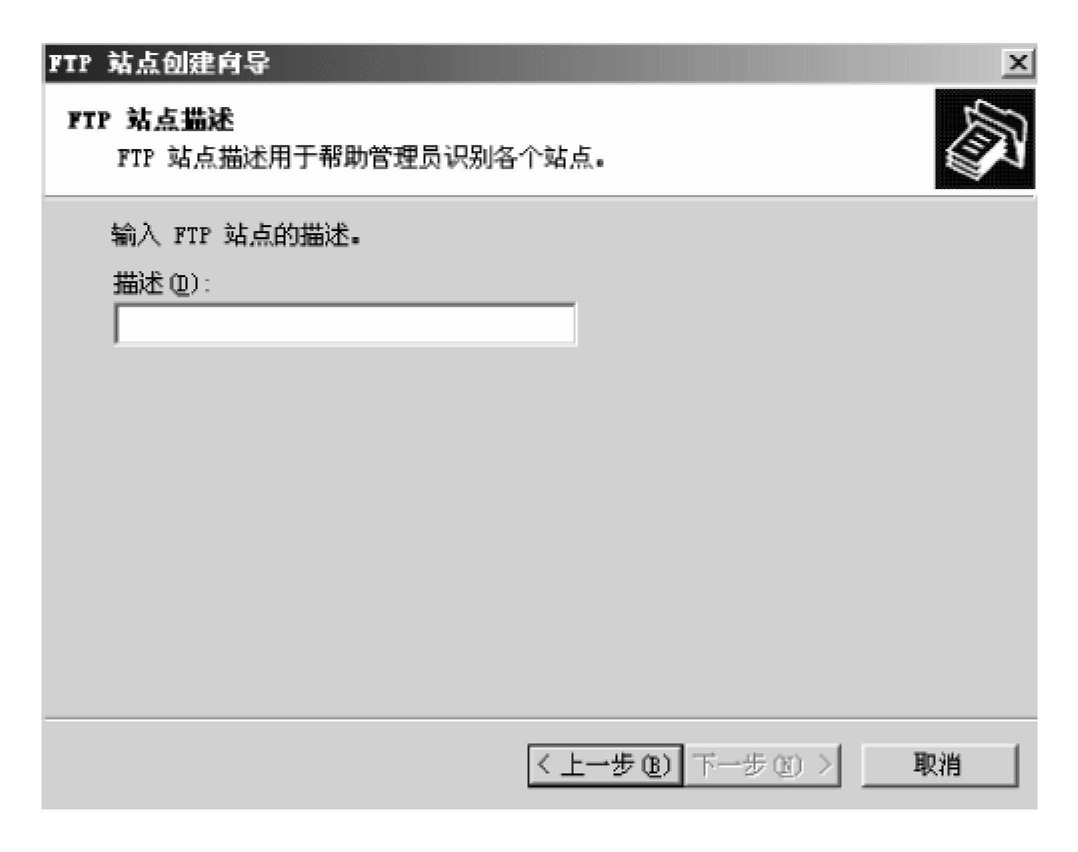


图 5-6 【FTP 站点创建向导】对话框—站点描述

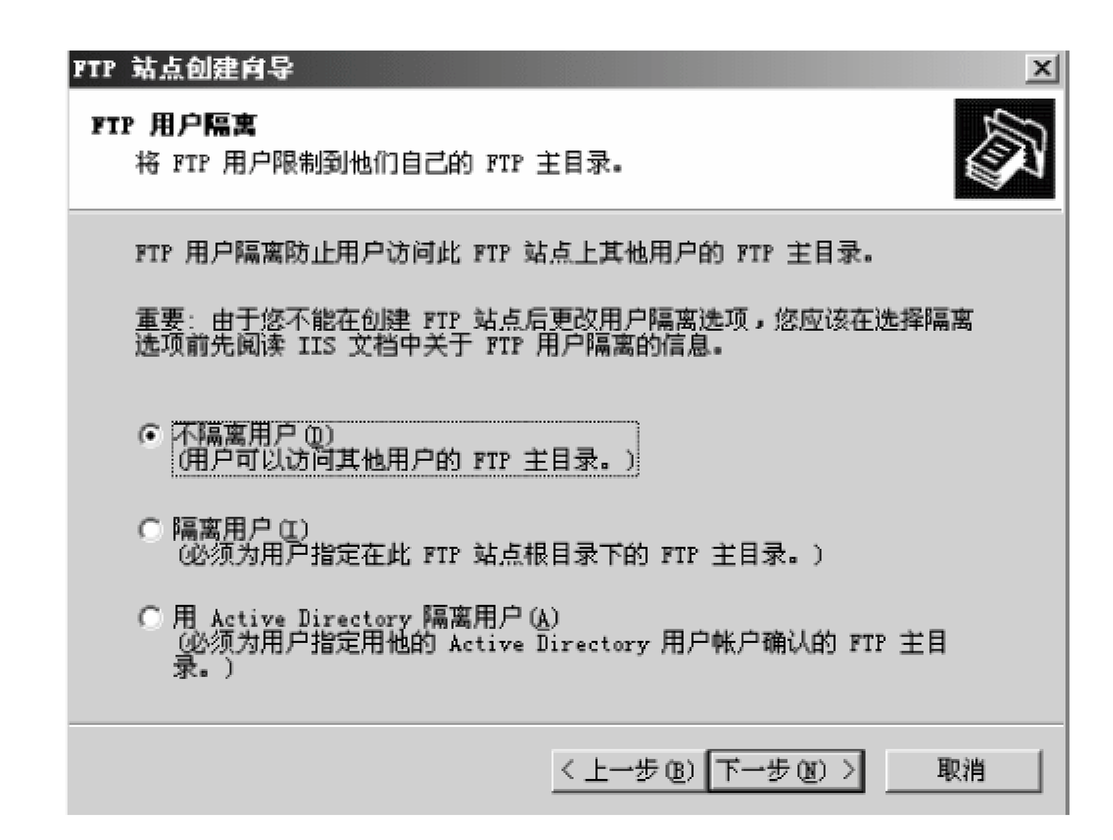


图 5-7 【FTP 站点创建向导】对话框—用户隔离

(3) 单击【下一步】按钮，设置 FTP 站点的路径和站点权限。这样就完成了 FTP 用户隔离功能的站点设置。

与 Windows 2000 Server 中创建的 FTP 站点相比，基于 Windows Server 2003 的 FTP 站点无论在安全性还是可管理性等方面都要胜出一筹，尤其是利用 Windows Server 2003 提供的“隔离用户”方式可以创建不同应用需求的 FTP 站点。

5.4 配置 FTP 站点

5.4.1 更改 FTP 站点的主目录

FTP 站点的主目录可以修改，操作步骤如下：

(1) 在【Internet 信息服务(IIS)管理器】窗口中选取要更改的 FTP 站点的名称，右击，在弹出的快捷菜单中选择【属性】命令，调出【默认 FTP 站点 属性】对话框，如图 5-8 所示。

(2) 选择【主目录】选项卡，修改主目录的路径。该路径可以是本地路径，也可以是网络中的资源。

(3) 在该对话框中修改站点的访问权限，各个权限描述如下：

- 读取。表示用户可以读取主目录内的文件，如下载文件等。
- 写入。表示用户可以在主目录内添加、删除、修改文件或目录。
- 记录访问。将连接到该 FTP 站点的信息记录到日志文件中。

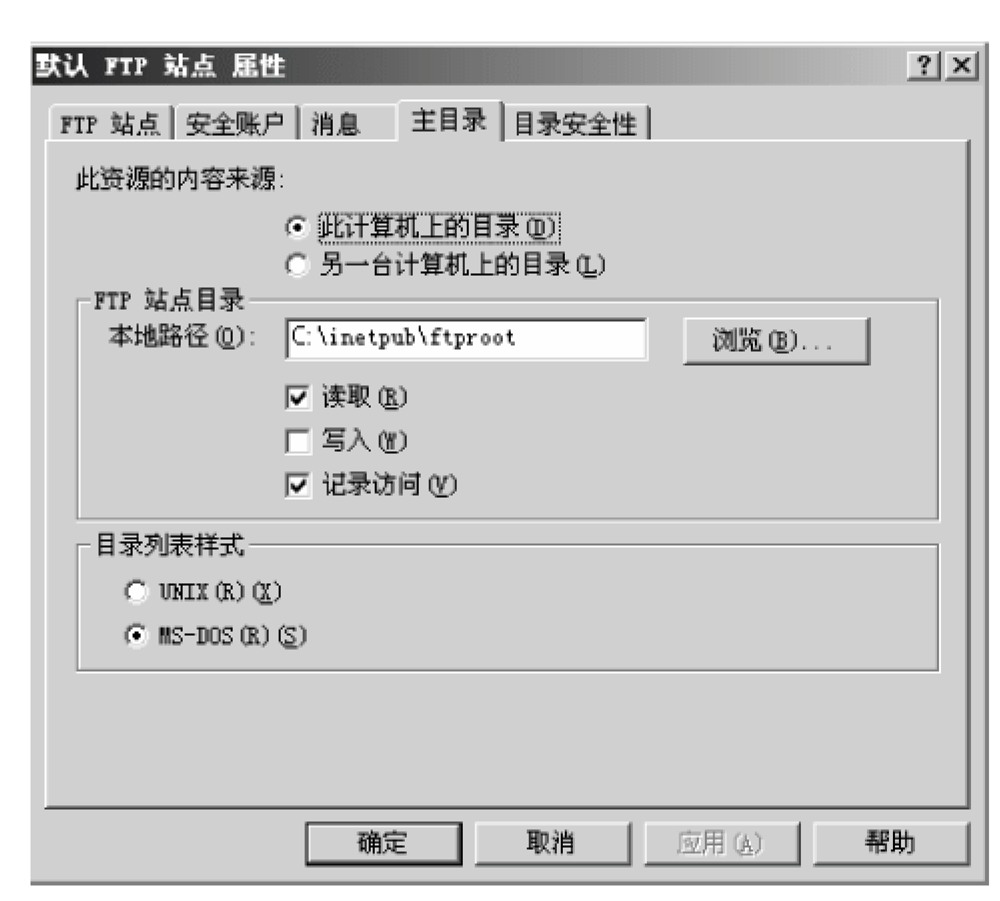


图 5-8 【默认 FTP 站点 属性】对话框



5.4.2　设置 FTP 站点的标识、连接限制及日志记录

选择【FTP 站点】选项卡，可以设置站点的标识、连接限制和日志记录等内容，如图 5-9 所示。

5.4.3　设置 FTP 站点的消息提示

在客户端登录 FTP 站点时，为了增强与客户端之间的信息沟通，可以为 FTP 站点设置消息提示。方法是在如图 5-10 所示的【消息】选项卡中进行设置。



图 5-9　【FTP 站点】选项卡



图 5-10　【消息】选项卡

5.4.4　设置用户身份验证

目前，用户访问网络中的大部分 FTP 站点时是不需要进行身份验证的，即用户使用匿名方式访问这些站点。但是，也有一些 FTP 站点在用户访问时需要输入正确的用户名和密码，否则无法登录访问。

在【Internet 信息服务(IIS)管理器】窗口中选取要设置的 FTP 站点，右击，在弹出的快捷菜单中选择【属性】命令，从打开的对话框中选择【安全账户】选项卡，如图 5-11 所示。



图 5-11　【安全账户】选项卡

5.4.5　利用 IP 地址来限制客户端的 FTP 站点连接

实际应用中有的 FTP 站点对访问者的 IP 有限制，比如说各大高校内部都有许多 FTP 站点，可以提供许多有用的资料。但这种站点一般都限制访问者的 IP 为本校的或者教育网



的 IP 才可以访问。如果要实现这种应用,操作步骤如下:

在【Internet 信息服务(IIS)管理器】窗口中选取该 FTP 站点名称后右击,从弹出的快捷菜单中选择【属性】命令,在打开的对话框中选择【目录安全性】选项卡。从中可进行设置,如图 5-12 所示。

5.4.6 查看 FTP 站点的当前连接用户

如果管理员要查看 FTP 站点当前有多少用户在线,可以按下列步骤操作:

(1) 在【Internet 信息服务(IIS)管理器】窗口中选取要查看的 FTP 站点名称。

(2) 右击,从弹出的快捷菜单中选择【属性】命令。

(3) 在打开的对话框中选择【FTP 站点】选项卡。单击【当前会话】按钮,调出【FTP 用户会话】对话框,查看已登录的用户情况,如图 5-13 所示。



图 5-12 【目录安全性】选项卡



图 5-13 【FTP 用户会话】对话框

5.5 访问 FTP 站点

一般通过两大类方法访问 FTP 站点。一类是在浏览器的地址栏里直接输入 ftp://local,其中 local 可以替换为任意 IP 号或域名,这样就可以在浏览器中打开 FTP 站点了,但这种方式只支持单线程下载,并且经常出现连接超时的问题,使用起来不是很方便,所以用途也不广泛。第二种方法是通过 FTP 客户端软件连接 FTP 站点,这种 FTP 客户端软件有 FlashFXP、CuteFTP、迅雷 FTP 探针等很多种,其中使用最方便的当属 FlashFXP,它的上传或下载过程中的断点续传能力最强,程序运行最稳定,且占内存最小,应用非常广泛。图 5-14 所示就是 FlashFXP 软件的主界面。

在图 5-14 所示对话框的【服务或 URL】文本框中输入一个 IP 或域名,在【用户名】文本框中输入一个合法的用户名,在【密码】文本框中输入对应的正确密码,然后单击【连接】按钮





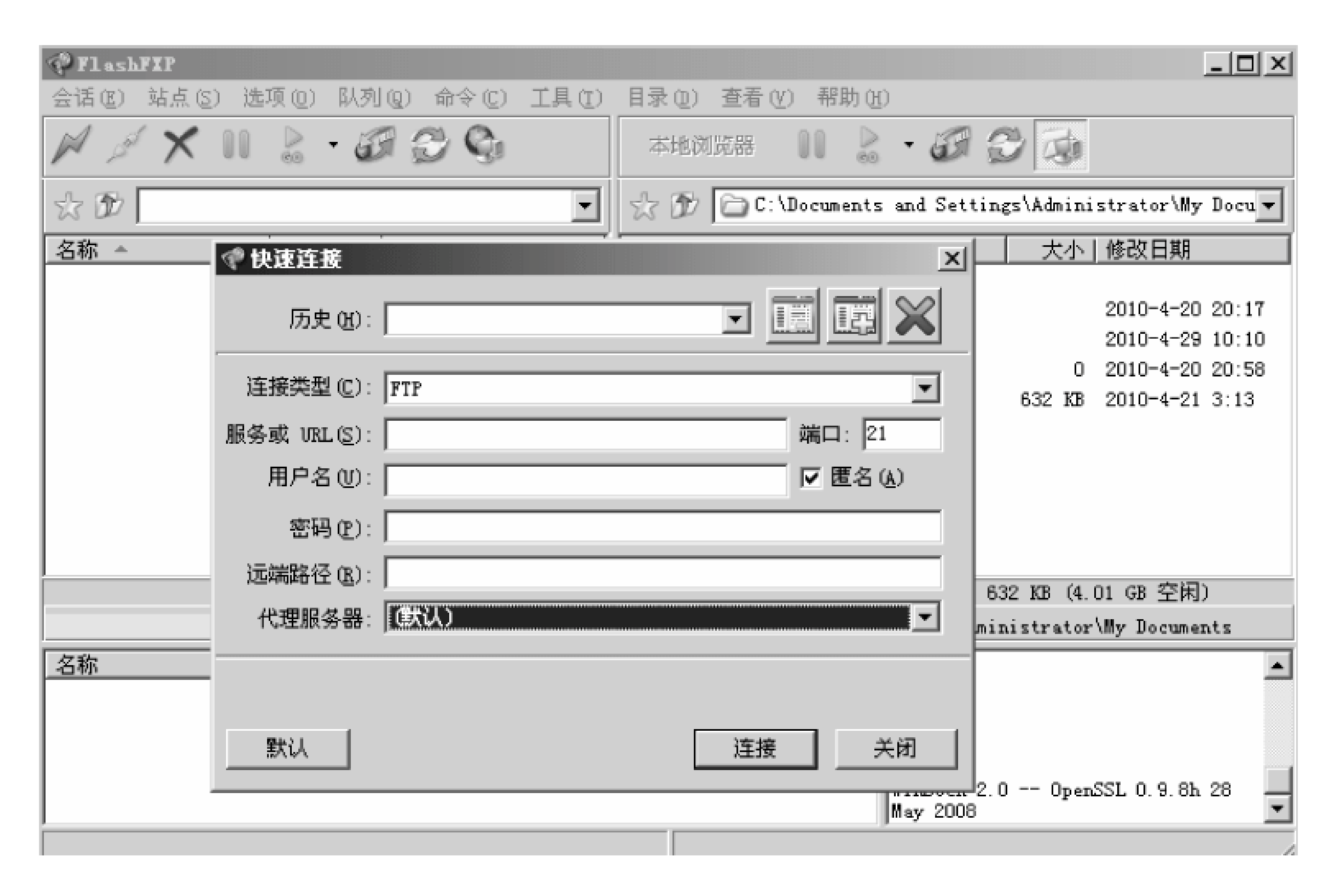


图 5-14　FlashFXP 软件的主界面

就可以登录到远程 FTP 服务器。登录后的主界面是一个资源管理器的样式，使用非常方便，在此就不再赘述了。

5.6　安装 Serv-U 服务器

本书中用到的 Serv-U 软件是 Serv-U 6.4。其安装步骤如下：

(1) 运行下载好的 Serv-U 安装程序，开始安装 Serv-U 服务器软件，如图 5-15 所示。

(2) 单击 Next 按钮，开始按照向导安装 Serv-U 服务器软件。其中安装目录建议不要选择默认的安装目录，最好更改为一个不容易被猜测到的目录，如图 5-16 所示。

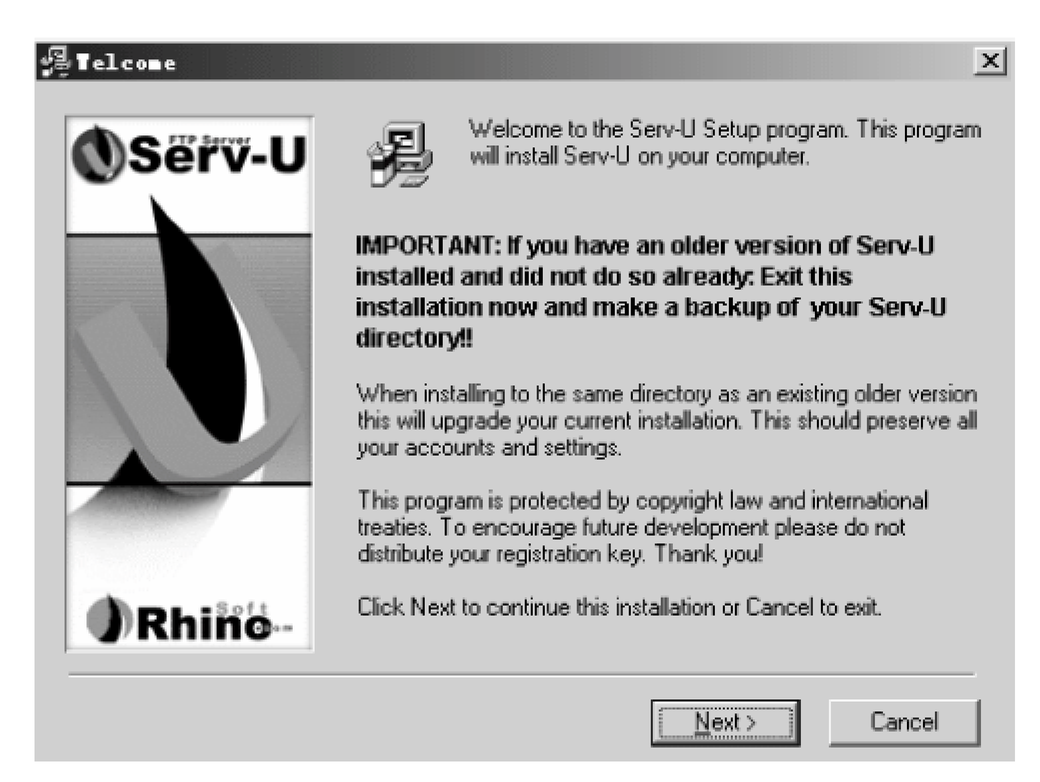


图 5-15　Welcome 对话框

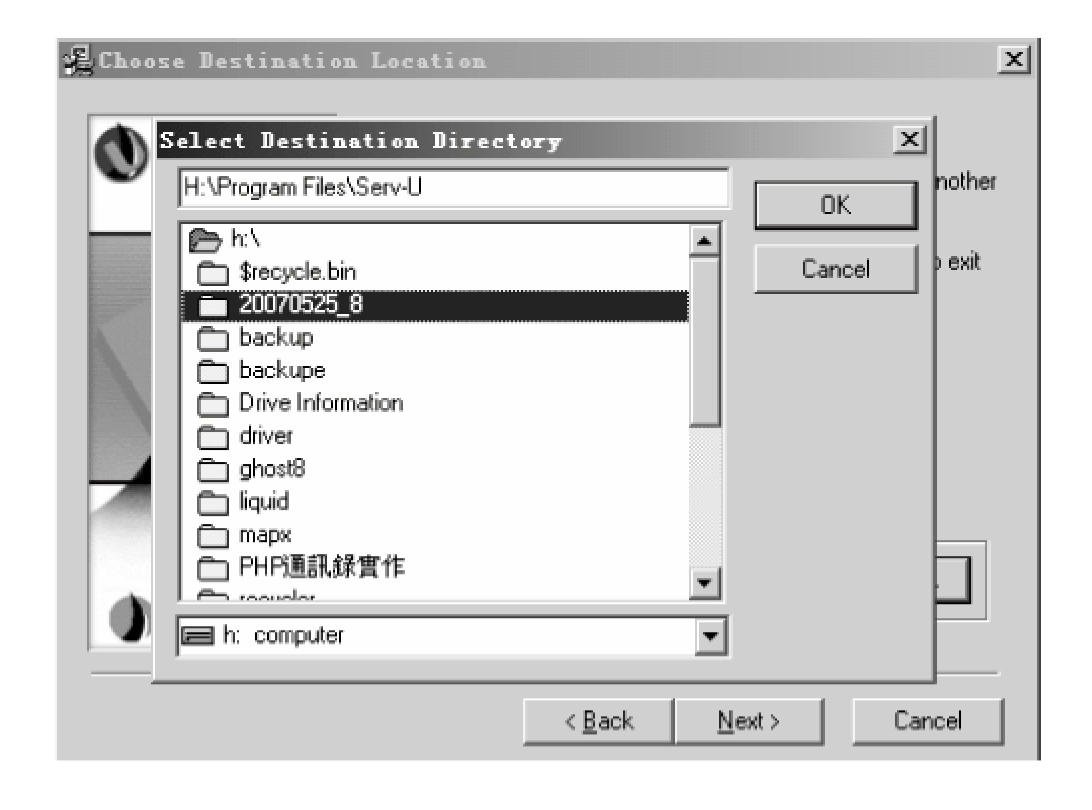


图 5-16　Choose Destination Location 对话框

(3) 设置服务器 IP。单击 Next 按钮，开始对 Serv-U 服务器进行必要的属性设置，如图 5-17 所示。在 Your IP address 文本框中输入服务器的 IP 号。

(4) 设置服务器名称。在图 5-18 所示对话框的 Domain name 文本框中输入对应的服务器名称。



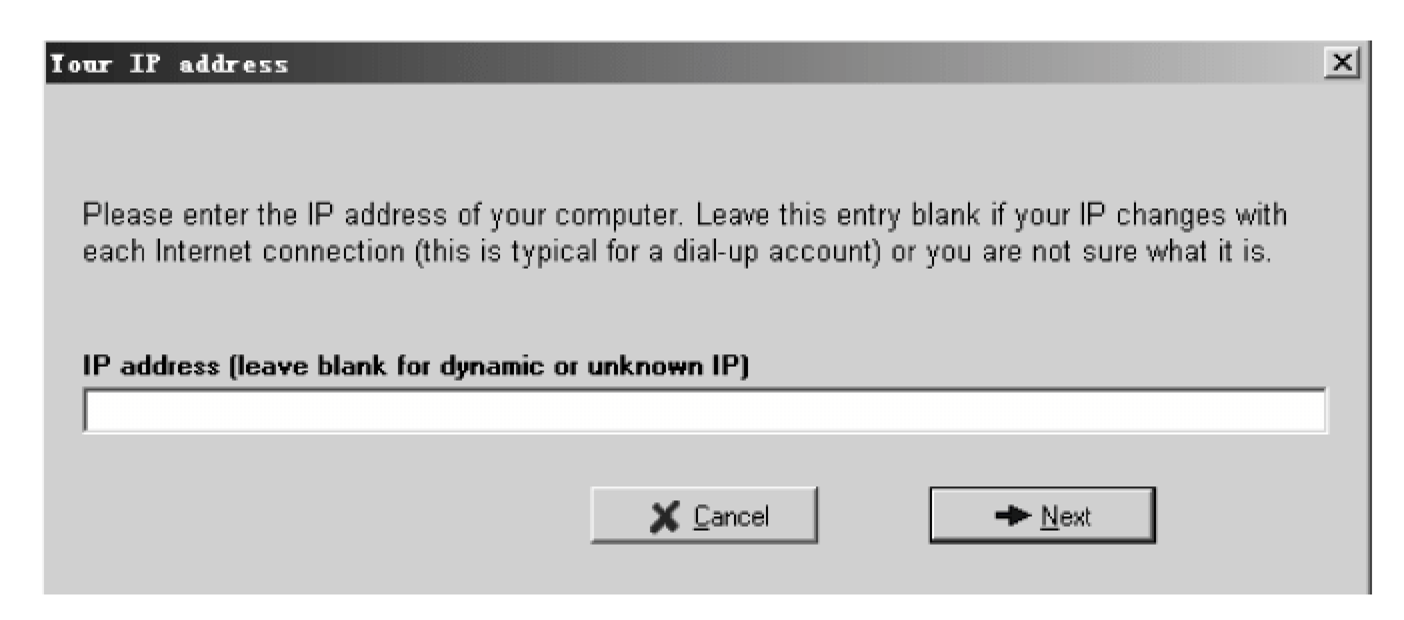


图 5-17　Your IP address 对话框

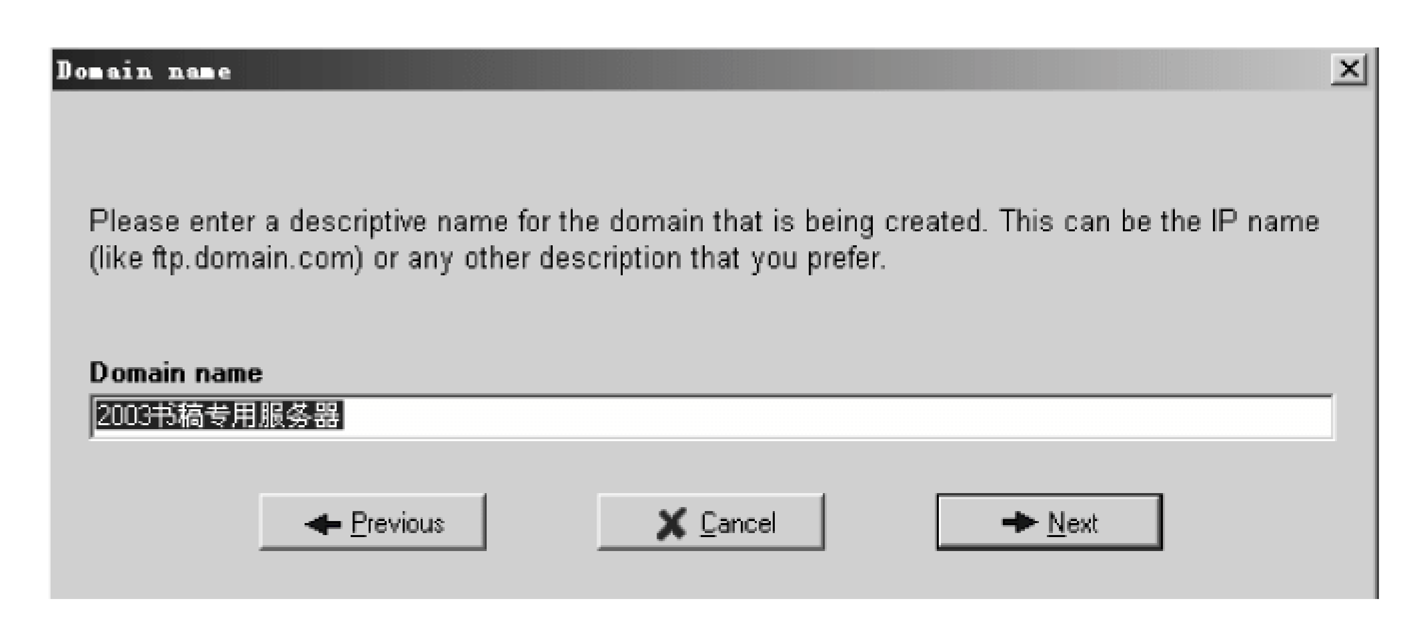


图 5-18　Domain name 对话框

(5) 安装为系统服务。在图 5-19 所示的对话框中,选中 Yes 按钮。

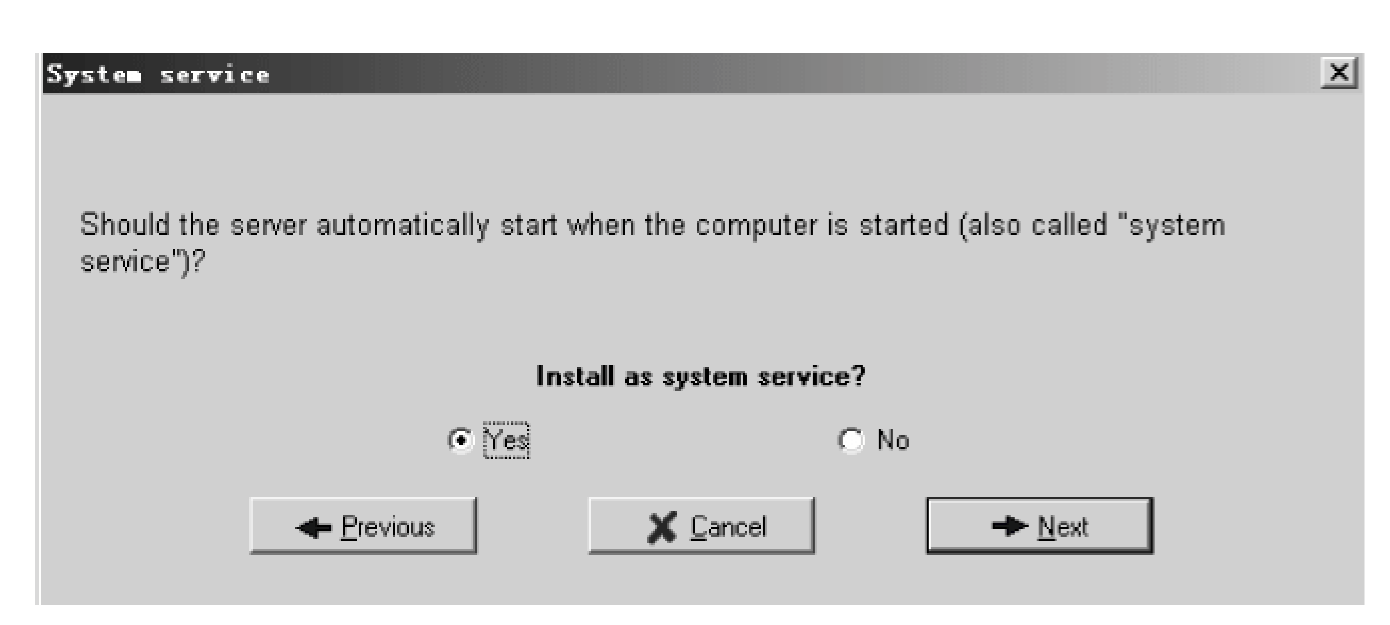


图 5-19　System service 对话框

(6) 设置登录用户信息。为了让 FTP 服务器更安全,一般不允许匿名用户登录,如图 5-20 所示,即要选中 No 按钮。然后单击 Next 按钮,为 FTP 服务器设置其他账号并建立强密码。最后单击 Finish 按钮完成 Serv-U 的基本设置,如图 5-21 所示。



图 5-20　Anonymous account 对话框





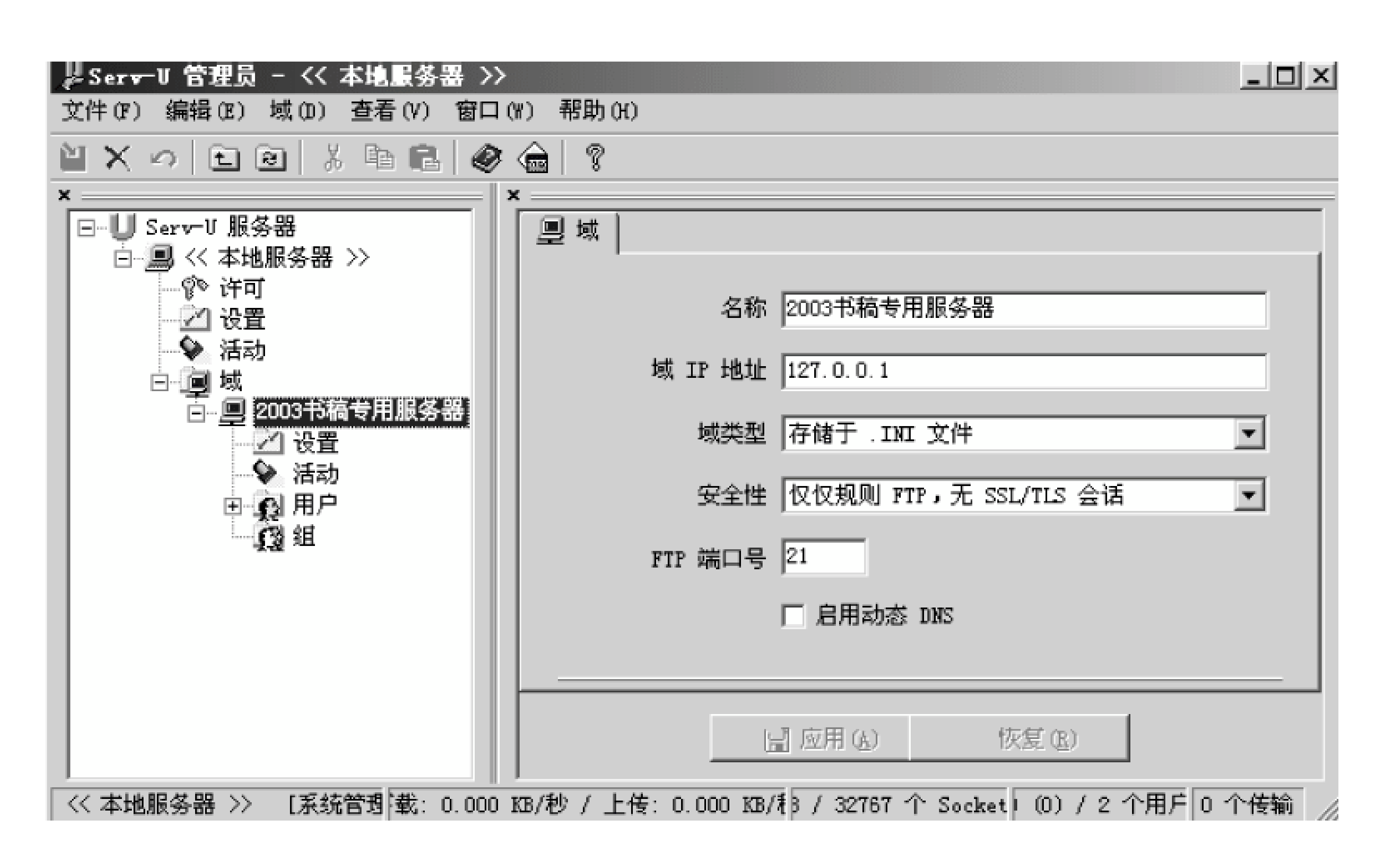


图 5-21　【Serv-U 管理员】窗口

5.7　打造 SSL 安全加密的 Serv-U 服务器

5.7.1　更改默认管理账号

Serv-U 6.4 有一个本地提权漏洞。ServUAdmin.exe 是 Serv-U 的管理界面，由于 ServUAdmin.exe 对异常的不正确处理，导致在 Serv-U 被注册为系统服务的情况下，本地普通用户可以进行权限提升，得到超级用户权限。要解决这个问题需要对 Serv-U 做一些必要的安全设置。

打开 Serv-U 主界面后，首先要更改的是管理密码。因为第一次使用是没有密码的，也就是说原来的密码为空。单击图 5-21 中的“设置/更改密码”按钮，调出【设置或更改管理员密码】对话框，从中可更改默认管理密码，如图 5-22 所示。

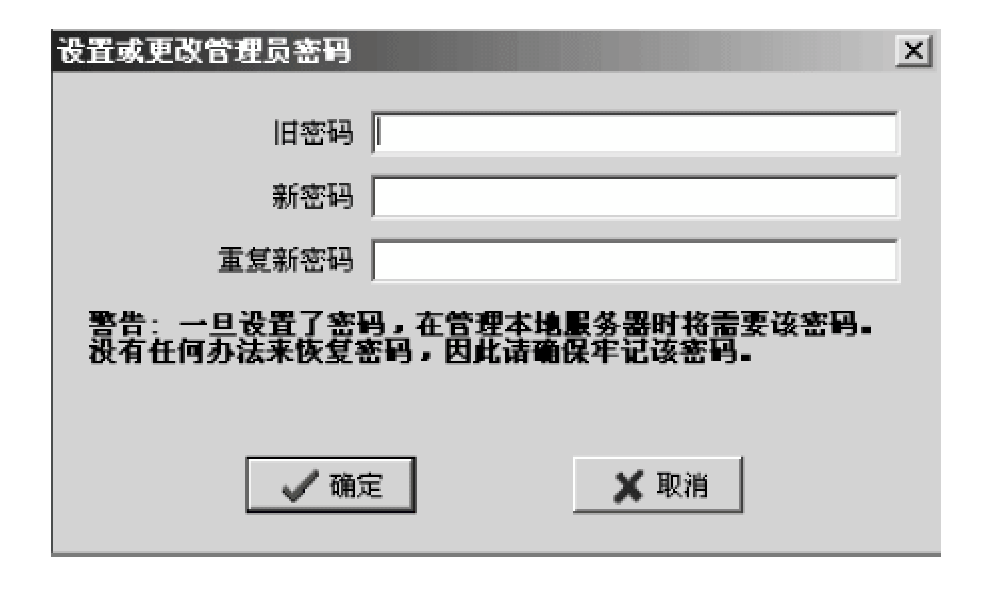


图 5-22　【设置或更改管理员密码】对话框

其中，在【旧密码】文本框中不用输入字符，直接在下面的【新密码】和【重复新密码】文本框中输入同样的密码，单击【确定】按钮就可以了。这里建议设置一个包括字符、数字、特殊符号的足够复杂的密码，以防别人暴力破解。自己记不住也没有关系，只要把 ServUDaemon.ini 里的 LocalSetupPassword＝ 这一行清除并保存，就可以把刚设置的管理密码清除了。

同时还要注意设置 Serv-U 安装目录的权限，不要让 IIS 匿名用户有读取的权限，否则黑客下载 ServUDaemon.ini 和 ServUAdmin.ini 这两个文件，同样可以分析出管理密码，然后进行提权。



5.7.2 建立启动 Serv-U 服务的非系统用户

下面开始对 Serv-U 进行安全设置。操作步骤如下：

(1) 在【计算机管理】窗口中建立一个 Windows 系统账号 ServerFTP，密码需要足够复杂。建好账号以后，双击建好的用户，编辑用户属性，从【隶属于】列表框中删除 Users 组，如图 5-23 所示。

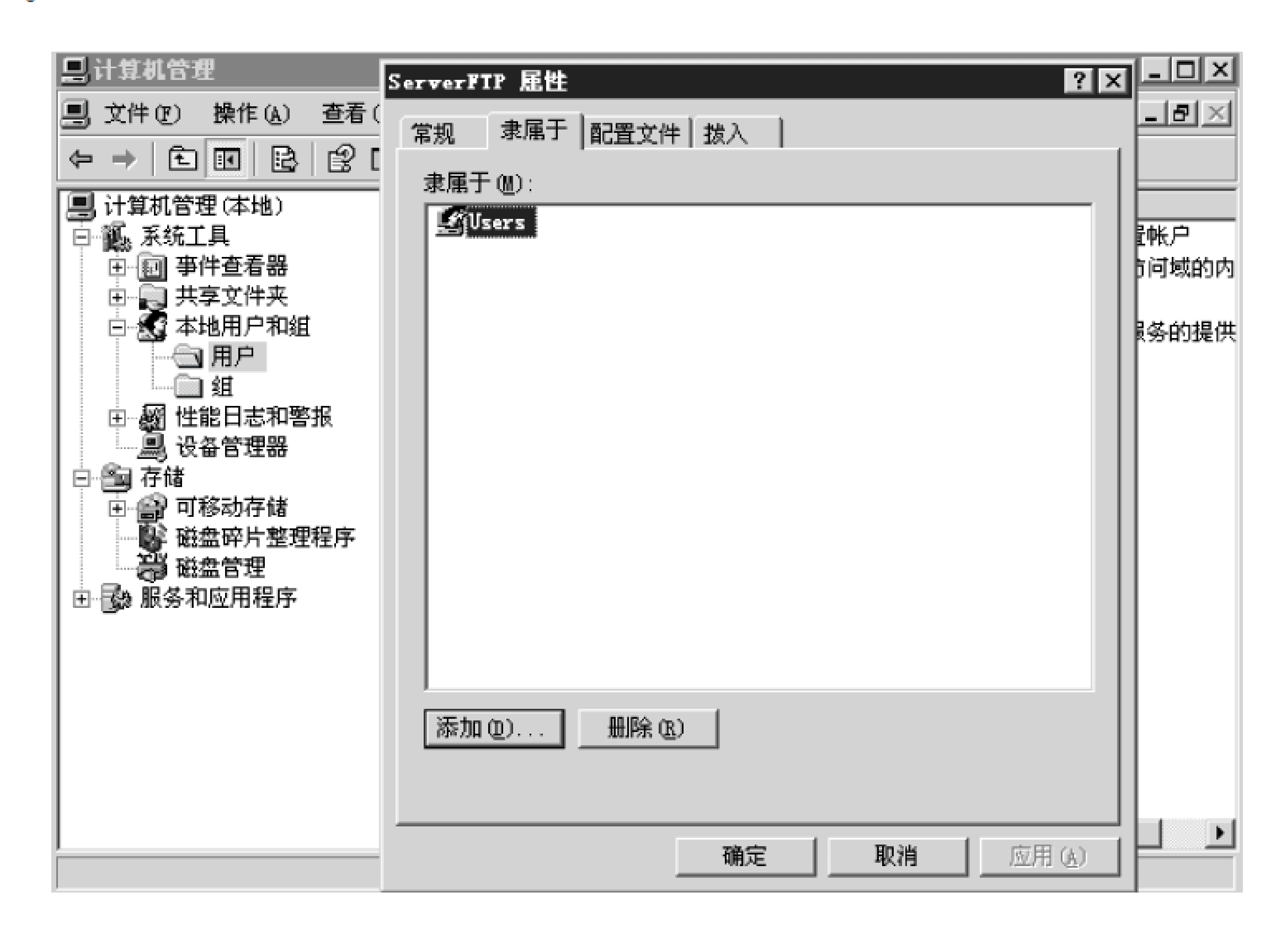


图 5-23 【计算机管理】窗口

(2) 设置用该新建账号 ServerFTP 替换掉原来的 Serv-U 服务的启动账号。依次选择【开始】→【程序】→【管理工具】→【服务】，右击【Serv-U FTP Server 服务】，从弹出的快捷菜单中选择【属性】命令，调出该服务的属性对话框，如图 5-24 所示。

(3) 选择【登录】选项卡，进入登录账号选择界面。选择刚才建立的系统账号名 ServerFTP，并在下面的【密码】和【确认密码】文本框中分别输入该账号的密码，然后单击【应用】按钮，完成 Serv-U 服务启动账号的替换。



图 5-24 【Serv-U FTP Server 的属性】对话框

5.7.3 更改 Serv-U 对应的注册表项与安装目录的权限

经过上述设置，将 Serv-U 的启动服务替换为 ServerFTP 用户后，Serv-U 服务程序仍没法运行，还需要在注册表里将 Serv-U 程序对应的注册表项的权限也赋给 ServerFTP 用户



才可以。操作步骤如下：

（1）一般 Serv-U 中的默认域信息是存在 ini 文件中的，此处为了安全设置，需要将域信息存在系统注册表中。先使用 Serv-U 的管理程序建立一个新的域，在这个新域里建立一个账号，然后在【域类型】列表框中选择"存储于计算机注册表"，如图 5-25 所示。

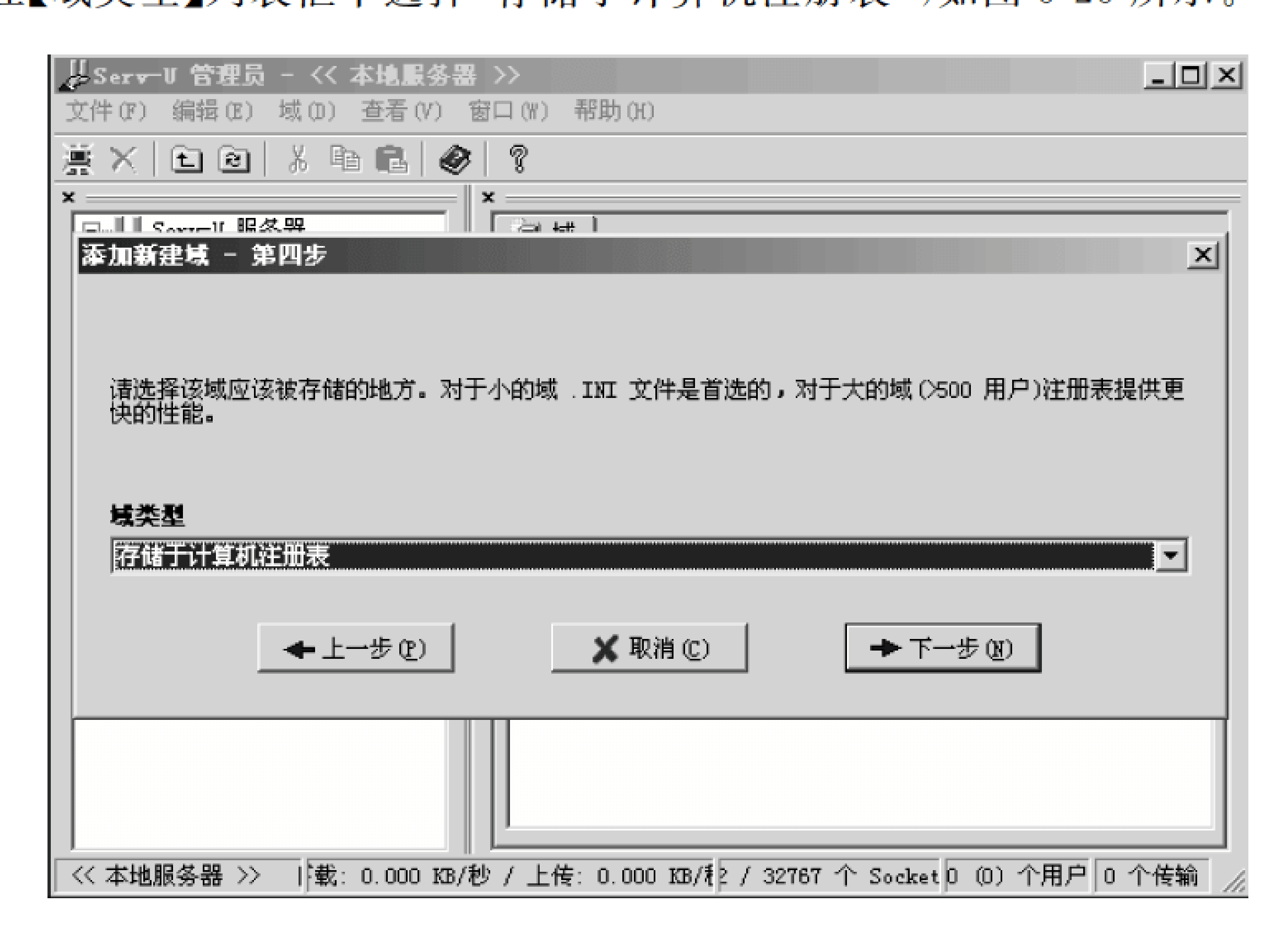


图 5-25　新建域

（2）打开注册表来设置相应的权限，否则 Serv-U 是没法启动的。依次选择【开始】→【运行】，输入 regedit，调出系统注册表。

（3）在注册表里找到 HKEY_LOCAL_MACHINE\SOFTWARE\Cat Soft 表项，右击该表项，从弹出的快捷菜单中选择【权限】命令，调出如图 5-26 所示的对话框。然后单击【高级】按钮，在调出的对话框中取消【允许父项的继承权限传播到该对象和所有子对象，包括那些在此明确定义的项目】复选框，最后单击【应用】按钮退出该对话框。

（4）在图 5-26 中删除所有用户名后，单击【添加】按钮，增加系统管理员 Administrator 和新建的 ServerFTP 账号并给予完全控制权限，这样注册表里的权限设置就完成了。

（5）下面进行安装目录的权限设置。右击 Serv-U 的安装目录，从弹出的快捷菜单中选择【属性】命令，调出该文件夹的属性对话框。在对话框中选择【安全】选项卡，对安装目录进行权限设置。这里建议只保留系统管理员账号和 ServerFTP 账号，并给予 ServerFTP 账号除了完全控制外的所有权限。经过上述设置之后，服务器上的 Serv-U FTP Server 服务就可以正常启动了。

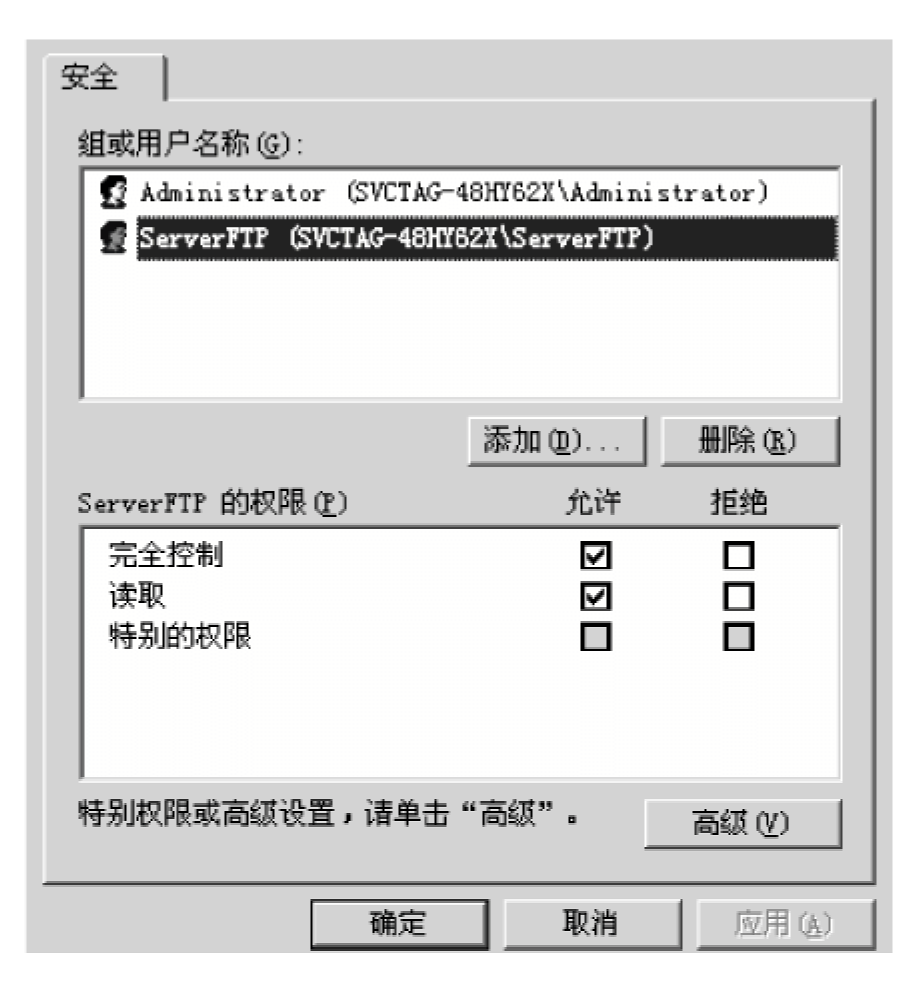


图 5-26　为 Serv-U 注册表项设置权限



5.7.4 更改站点主目录的目录权限

到目前为止,服务器的 FTP 用户还是没有权限登录站点,还需进行最后一个步骤,就是设置 FTP 站点主目录的目录权限。假设 FTP 站点主目录为 D:\download。那么就右击 download,从弹出的快捷菜单中选择【属性】命令,调出该文件夹的属性对话框。在对话框中选择【安全】选项卡,对 download 目录进行权限设置。这里建议保留 Administrator 管理员账号和 IIS 用户,再加入 FTP 服务对应的 ServerFTP 账号,切记 SYSTEM 账号一定要删掉。

这样设置的原因是现在已经用 ServerFTP 账号启动了 Serv-U 服务,而不是用 SYSTEM 权限启动的,此时 SYSTEM 已经没用。这样就算真的有黑客成功溢出也得不到 SYSTEM 权限。

另外,一般情况下禁止对 FTP 服务的匿名访问。如果允许匿名访问,该匿名账户就有可能被利用来获取更多服务器的有关信息,进一步展开社会工程学攻击,以致对系统造成危害。

5.7.5 仔细设置账户权限

一般来说,不需要将多余的权限授予用户。因此,只要根据账户类型需要,在【目录访问】选项卡中选择相应的操作类型即可。但是有一点需要注意的是,不管是什么用户,建议都不要授予其“执行”权限,如图 5-27 所示。



图 5-27 设置账户权限

5.7.6 启用 SSL

一般的 FTP 服务器是以明文方式传输数据的,安全性极差,信息很容易被盗。虽然它提供了 SSL 加密功能,默认情况下也是没有启用的,如最常用的 Serv-U FTP 服务器。所





以，为了保证特殊环境下的数据安全，有必要启用 SSL 功能，提高服务器数据传输的安全性。下面以 Serv-U 为例进行介绍。操作步骤如下：

（1）创建 SSL 证书。要想使用 Serv-U 的 SSL 功能，需要 SSL 证书的支持才行。虽然 Serv-U 在安装之时就已经自动生成了一个 SSL 证书，但这个默认生成的 SSL 证书在所有的 Serv-U 服务器中都是一样的，非常不安全，所以需要手工创建一个自己独特的 SSL 证书。

（2）在【Serv-U 管理员】窗口中，依次选择【本地服务器】→【设置】，然后切换到【SSL 证书】选项卡，如图 5-28 所示。

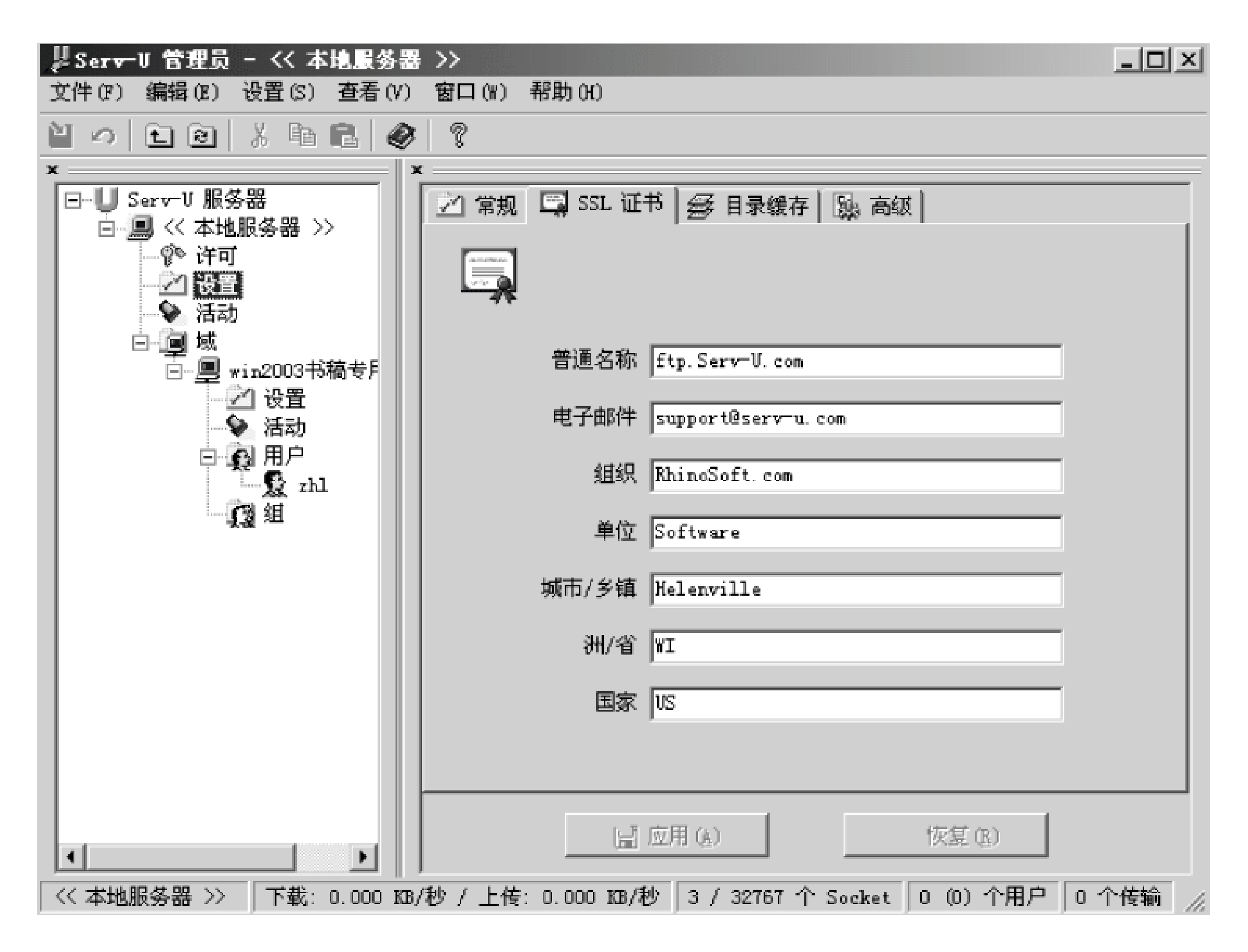


图 5-28　设置 SSL 证书

（3）创建一个新的 SSL 证书。在图 5-28 所示的【普通名称】文本框中输入 FTP 服务器的 IP 地址，接着可设置其他文本框的内容，如电子邮件、组织和单位等。根据用户的情况进行填写。

（4）完成所有内容的填写后，单击下方的【应用】按钮即可。这时 Serv-U 就会生成一个新的 SSL 证书。

（5）虽然为 Serv-U 服务器创建了新的 SSL 证书，但默认情况下，Serv-U 是没有启用 SSL 功能的。要想利用该 SSL 证书，首先要启用 Serv-U 的 SSL 功能才行，即要启用 Serv-U 服务器中域名为“win2003 书稿专用服务器”的 SSL 功能。

（6）在【Serv-U 管理员】窗口中，依次选择【本地服务器】→【域】→【win2003 书稿专用服务器】，在右侧的【域】管理框中找到【安全性】下拉列表框。这里 Serv-U 提供了 3 种选项，分别是“仅仅规则 FTP，无 SSL/TLS 进程”。“ 允许 SSL/TLS 和规则进程”和“只允许 SSL/TLS 会话”，默认情况下，Serv-U 使用的是“仅仅规则 FTP，无 SSL/TLS 进程”，即是没有启用 SSL 加密功能的。

（7）在【安全性】下拉列表框中选择【只允许 SSL/TLS 会话】选项，然后单击【应用】按钮，即可启用域的 SSL 功能，如图 5-29 所示。





图 5-29 启动 SSL

提示：启用了 SSL 功能后，Serv-U 服务器使用的默认端口号就不再是 21 了，而是 990。这一点在登录 FTP 的时候一定要留意，否则就会无法成功连接 Serv-U 服务器。

5.7.7 认真查阅日志

用户访问 FTP 服务器时，Serv-U 都会忠诚地做下翔实的记录，这些记录中包括用户访问的 IP 地址、连接时间、断开时间、上传和下载的文件等。在管理窗口左侧选择要查看的域，然后再选择【活动】项，在右侧选择【域日志】，这样就可以看到详细的日志信息了。通过这些日志信息可以判断是否有恶意攻击。

5.7.8 注意升级

每一次补丁的发布都会弥补一些缺陷，因此建议大家在可能的情况下需要关注安全新闻，注意打补丁、及时升级。这同样是网络安全中通用的一条法则。

至此，FTP 服务器设置全部结束。服务器上的 FTP 服务器主要是为 Web(IIS)服务器做文件管理和维护使用。经过这样配置之后，FTP 与 IIS 使用不同的访问账号，Web 访问用户不管通过 FSO 或木马，都不可能访问 Serv-U 的安装目录，并且 Web 站点主目录可以不给予 SYSTEM 权限，所以就算黑客提权成功也同样访问不了 Web 目录。比如说，即使网站脚本程序有 SQL 注入漏洞并且是 sa 权限的，黑客也不能备份 Shell 到 Web 目录。经过上述层层设置之后，可以大幅提升服务器的整体安全性。



5.8　使用 SSL 加密连接 Serv-U 服务器

启用 Serv-U 服务器的 SSL 功能后，就可以利用此功能安全传输数据了，但 FTP 客户端程序必须支持 SSL 功能才行。

如果直接使用 IE 浏览器进行登录则会出现错误，这是因为 IE 浏览器不支持 SSL 协议传输，需要借助第三方 FTP 客户端程序来连接。这里以 FlashFXP 为例，介绍如何成功连接到启用了 SSL 功能的 Serv-U 服务器。操作步骤如下：

（1）运行 FlashFXP 程序后，选择【快速连接】命令，弹出【快速连接】对话框，如图 5-30 所示。在【服务器或 URL】文本框中输入 Serv-U 服务器的 IP 地址，在【端口】文本框中一定要输入 990，这是因为 Serv-U 服务器启用 SSL 功能后，端口号就从 21 变为 990。

（2）输入可以正常登录 FTP 服务器的用户名和密码。

（3）切换到 SSL 选项卡，选中【隐式 SSL】单选按钮，这一步骤非常关键。最后单击【连接】按钮，进行 FTP 连接，如图 5-31 所示。



图 5-30　【快速连接】对话框—设置用户名、密码

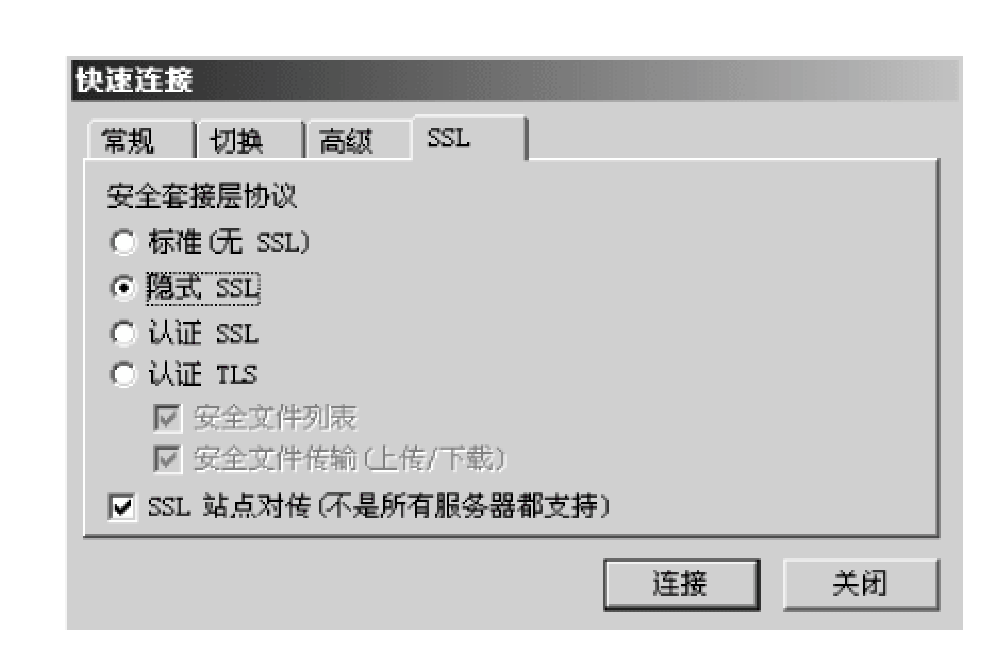


图 5-31　【快速连接】对话框—选择 SSL

（4）当用户第一次连接到 Serv-U 服务器时，FlashFXP 会弹出【证书】对话框，如图 5-32 所示。这时用户只要单击【接受并保存】按钮，将 SSL 证书下载到本地后，就能成功连接到 Serv-U 服务器。以后和 Serv-U 服务器间的数据传送就会受到 SSL 功能的保护，不再是以明文形式传送，这样就不用再担心 FTP 账号被盗、敏感信息被窃取的问题了。在 FlashFXP 的下方也会看到一个小锁的标志，这代表当前传输是加密安全的传输。

通过设置使用 SSL 进行加密传输的 FTP 站点就可以有效地保护自己服务器上的资源，使其不会被别人随意偷窥了。只有通过认证的用户才能下载到自己中意的文件资源。

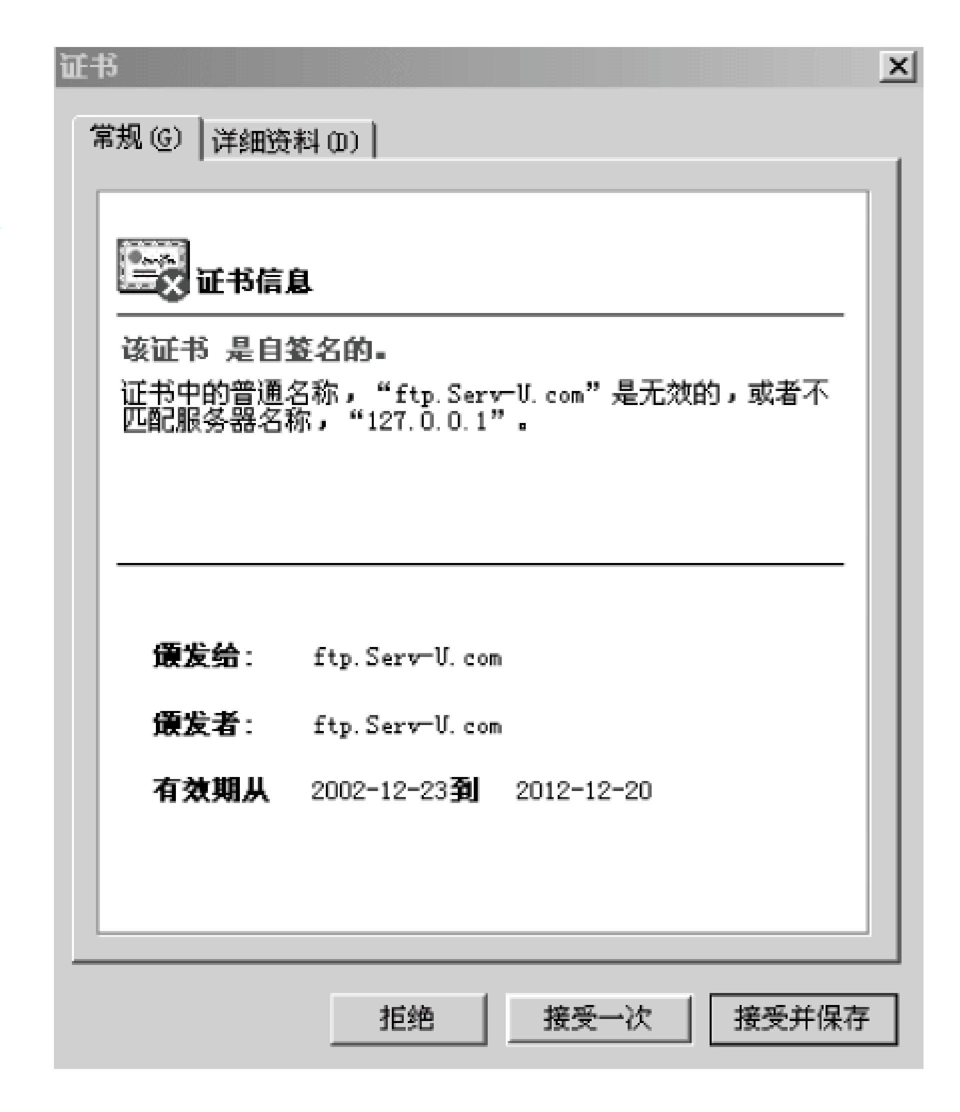


图 5-32　【证书】对话框



5.9 上机实战

本节主要练习 IIS 6.0 中 FTP 站点的创建过程。

5.9.1 安装 FTP 组件

安装 FTP 组件的步骤如下：

(1) 依次选择【开始】→【控制面板】→【添加/删除程序】命令，弹出【添加或删除程序】对话框。

(2) 在左侧窗格中，单击【添加/删除 Windows 组件】，弹出【Windows 安装程序】对话框。

(3) 不久系统会弹出【Windows 组件】对话框，从【组件】列表框中选中【应用程序服务器】复选框，然后单击【详细信息】按钮。

(4) 从【应用程序服务器的子组件】列表中，选中【Internet 信息服务(IIS)】复选框，然后单击【详细信息】按钮。

(5) 从【Internet 信息服务(IIS)的子组件】列表中选中【文件传输协议(FTP)服务】复选框，然后单击【确定】按钮。

(6) 单击【下一步】按钮，可能被提示插入 Windows Server 2003 家族光盘或输入网络使用安装路径。

(7) 单击【浏览】按钮选择好 Windows Server 2003 的安装路径。

(8) 接着系统配置组件完毕后，单击【下一步】按钮，系统会弹出一个对话框，表示已经完成了 FTP 组件的安装。

5.9.2 创建 FTP 站点

在 IIS 中，创建 FTP 站点的步骤如下：

(1) 在【Internet 信息服务(IIS)管理器】窗口的左侧，右击【FTP 站点】选项，从弹出的快捷菜单中依次选择【新建】→【FTP 站点】命令，如图 5-33 所示。

(2) 接着系统会弹出一个【FTP 站点创建向导】对话框。利用这个创建向导，可以创建一个新的 FTP 站点。

(3) 单击【下一步】按钮，弹出一个对话框让用户输入关于新 FTP 站点的描述。FTP 站点描述是用来帮助管理员识别 FTP 站点的，所以输入的网站描述要简单、易记，如图 5-34 所示。

(4) 单击【下一步】按钮，系统就会弹出【IP 地址和端口设置】对话框，要求用户输入 FTP 站点的 IP 地址、FTP 站点的 TCP 端口。其中 FTP 站点的 TCP 端口一般使用默认设置，如图 5-35 所示。

(5) 单击【下一步】按钮，系统会弹出【FTP 用户隔离】对话框。利用它，用户可以限制用户是否可以访问其他用户的 FTP 主目录，如果隔离用户，就必须为用户指定在 FTP 根目录的 FTP 主目录，如图 5-36 所示。

(6) 单击【下一步】按钮，系统会弹出【FTP 站点主目录】对话框，要求用户输入新建 FTP 站点内容主目录在本地磁盘上的路径，如图 5-37 所示。当然，也可以单击【浏览】按钮直接进行选择。



图 5-33　【Internet 信息服务(IIS)管理器】窗口

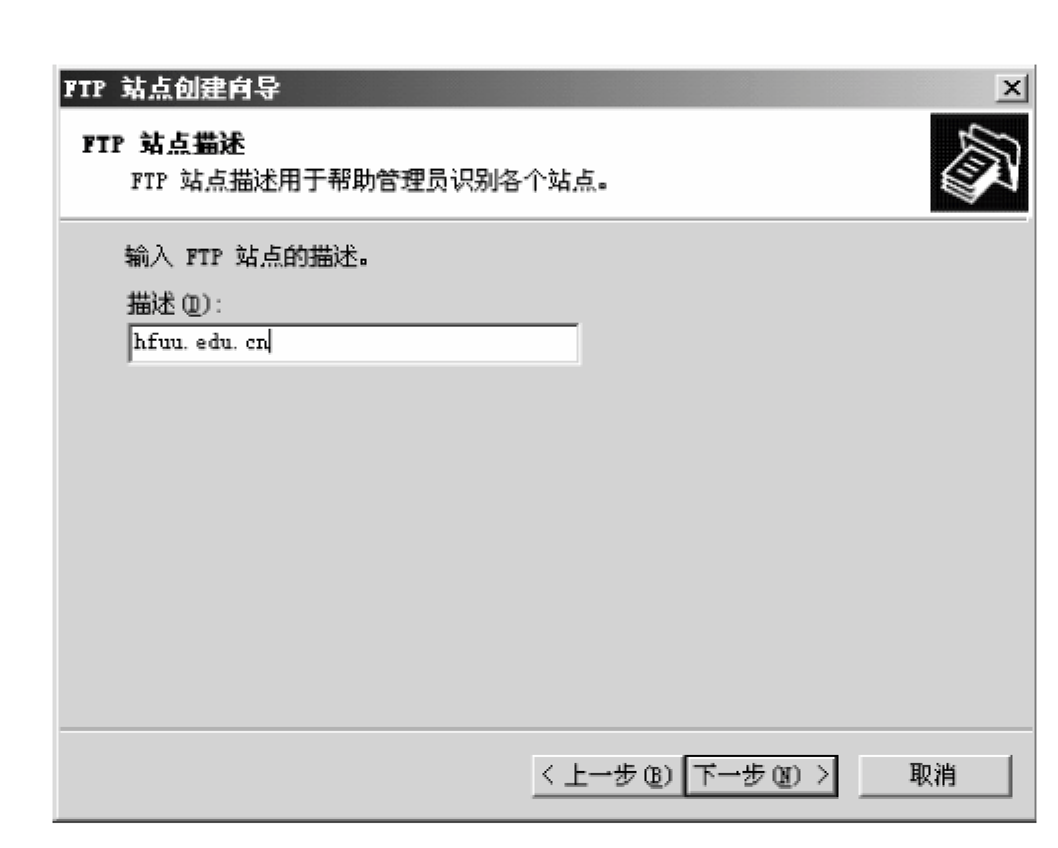


图 5-34　【FTP 站点创建向导】对话框

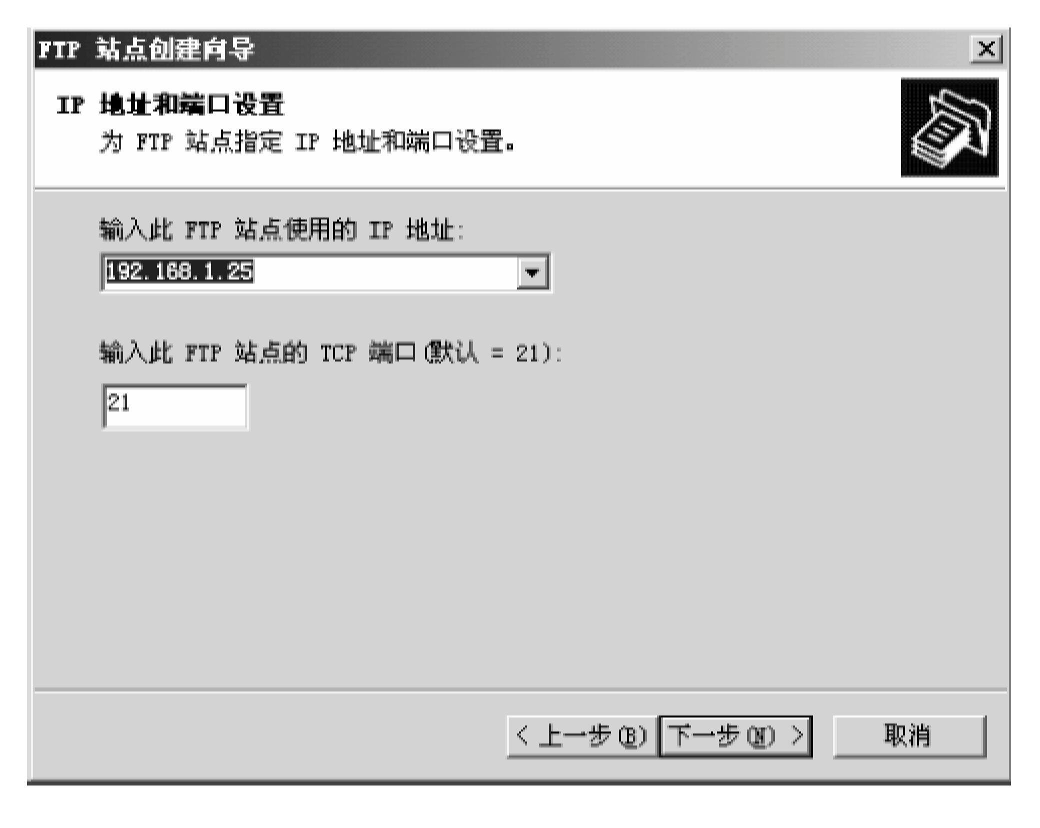


图 5-35　【IP 地址和端口设置】对话框

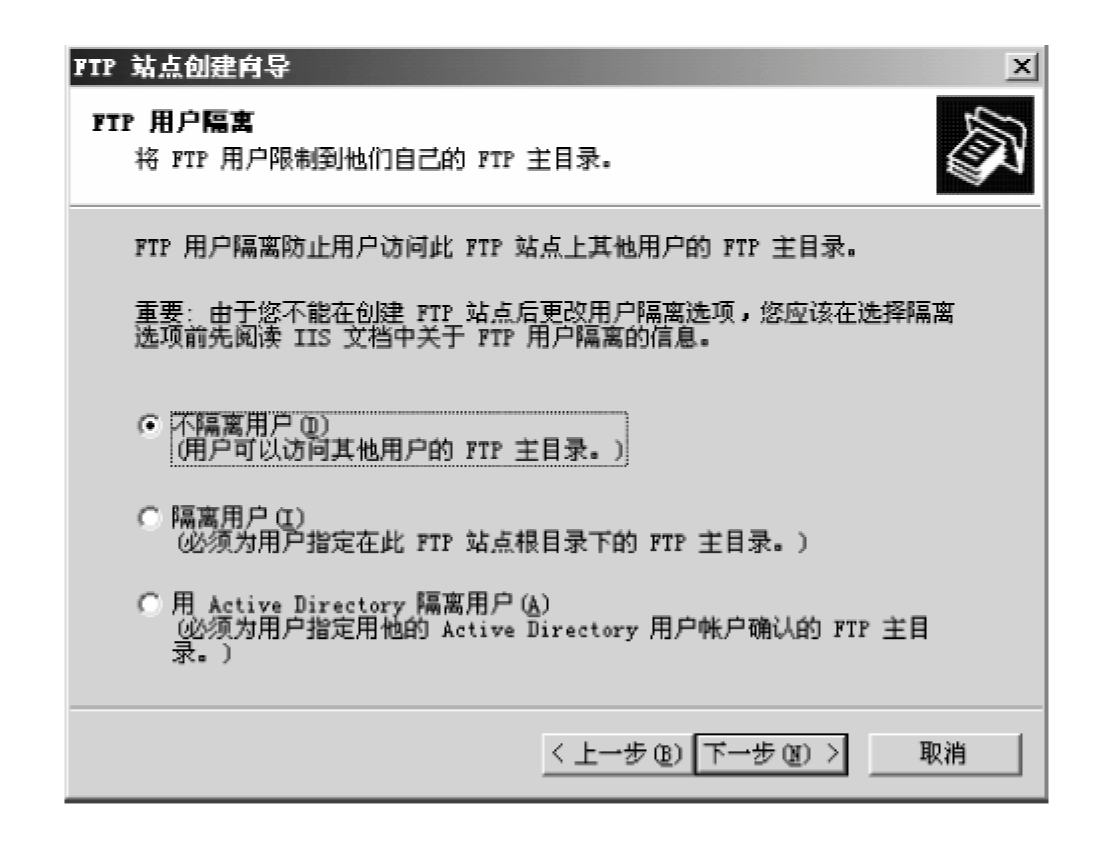


图 5-36　【FTP 用户隔离】对话框

（7）单击【下一步】按钮，弹出【FTP 站点访问权限】对话框。可以从中选择 FTP 站点访问权限，根据需要可以允许用户拥有读取或写入权限，如图 5-38 所示。



图 5-37　【FTP 站点主目录】对话框

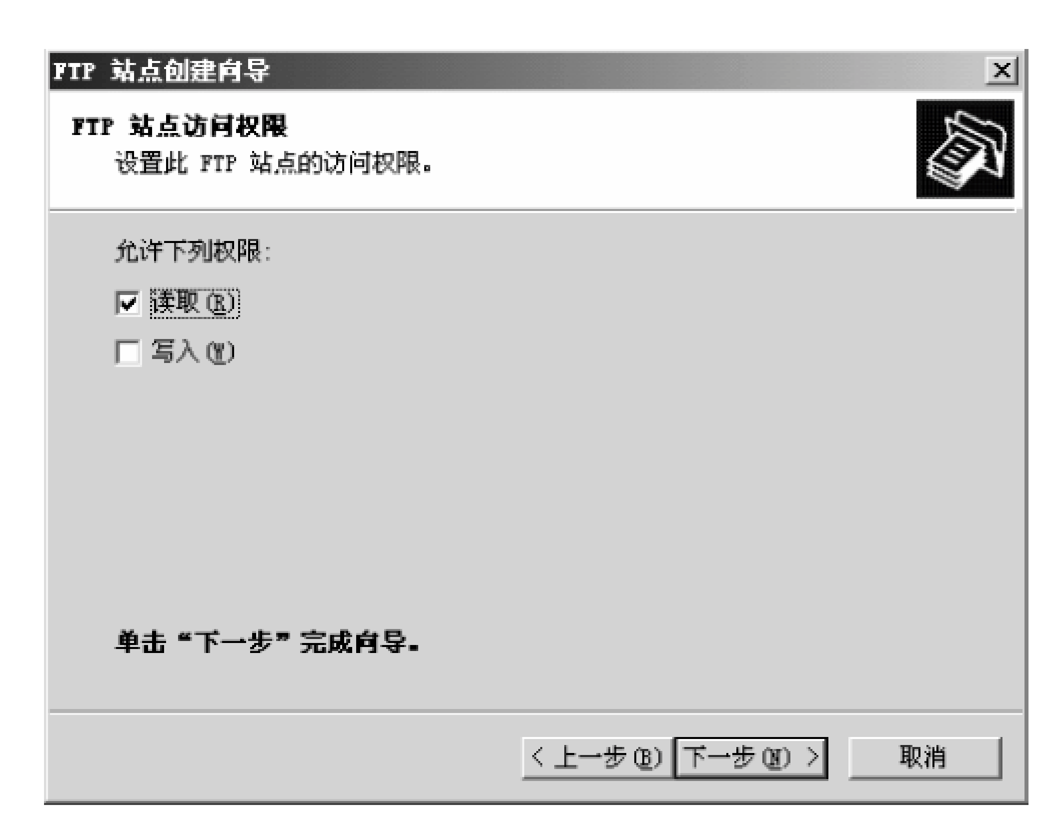


图 5-38　【FTP 站点访问权限】对话框



(8) 单击【下一步】按钮，系统会弹出一个对话框表示 FTP 站点已经成功创建。

5.10 疑难解答

1. IE 7 无法上传、下载 FTP 文件

IE 7 下不能登录 FTP 服务器下载文件，这种情况下可以修改一下注册表项，把 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_INTERNET_SHELL_FOLDERS 中的 iexplorer.exe 一项的值由 0 改为 1，然后重新开启 IE 7。这样 IE 7 就能像 IE 6 那样出现资源管理器的界面，此时就可以从 FTP 服务器中上传和下载文件了。

2. 如何更改 Internet Explorer 的客户端模式

启动 Internet Explorer 后依次选择【工具】→【Internet 选项】→【高级】，取消选中【为 FTP 站点启用文件夹视图】复选框，选中【使用被动 FTP(为防火墙和 DSL 调制解调器兼容性)】复选框，然后单击【确定】按钮。

3. Serv-U 无法看见目录中的中文名文件

打开 Serv-U 控制台，依次选择【限制和设置】→【FTP 设置】→【OPTS UTF8 命令】→【全局属性】→【高级选项】，取消选中【对所有收发的路径和文件名使用 UFT-8 编码】复选框。这样目录中原有的中文名文件就能看见了。

4. 如何设置 Serv-U 一用户多目录

打开 Serv-U 控制台，依次选择【用户属性】→【虚拟路径】，单击【添加】按钮为当前用户添加虚拟路径。这样该用户登录后，就能看到原来的主目录和新添加的虚拟目录了。

注意： 由于每个用户账户有一个"锁定在根目录"的限制，所以新加的虚拟路径要挂在该根目录下。例如，该用户的根目录是 D:\webftp，那么虚拟目录的虚拟路径就应该是 D:\webftp\virtualPath。

5. 如何使用"隔离用户"功能限制用户的 FTP 目录

在 IIS 6.0 发布之前，这一功能实现起来很麻烦。不过随着 Windows Server 2003 的发布，其 IIS 6.0 组件中集成的 FTP 服务子组件新增的"隔离用户"功能可以很好地解决上述问题。操作步骤如下：

(1) 首先在 Windows Server 2003 服务器中添加若干用户账户，并在某一个 NTFS 分区中创建一个文件夹作为 FTP 服务器的主目录。然后在该文件夹下创建一个名为 LocalUser 的子文件夹，最后在 LocalUser 文件夹下创建若干个和用户账户一一对应的个人文件夹。

(2) 新建 FTP 服务器，并在【FTP 站点向导】对话框中选择"隔离用户"模式。



(3) 这样以某一个用户的身份登录该 FTP 服务器时，则只能在属于该用户的目录中进行读写操作，且无法看到其他用户的目录。

提示： 如果在"隔离用户"的情况下依然希望允许匿名用户登录，则只需在 LocalUser 文件夹下面创建一个名为 Public 的文件夹，所有匿名用户将在该目录中进行读写操作。

6. 目录权限设置问题导致无法登录 FTP 服务器

在一台运行 Windows Server 2003 的服务器中用 IIS 6.0 配置了 FTP 服务器，当从其他计算机中使用合法的 FTP 账户和密码进行连接时却无法连接。

在排除物理连接和基本网络设置存在问题的情况下，可以考虑 FTP 服务器是否对用户启用了"读取"权限。如果没有开启"读取"权限，则会出现登录失败的情况。

解决的方法是在【Internet 信息服务(IIS)管理器】窗口中打开【FTP 站点属性】对话框。确认在【主目录】选项卡中选中【读取】复选框。然后切换至【目录安全性】选项卡，单击【授权访问】按钮，进一步确认客户端计算机的 IP 地址不在"拒绝访问"之列。

习　　题

1. 填空题

(1) 常用 FTP 命令中 GET 的功能是________。

(2) 常用 FTP 命令中 PUT 的功能是________。

2. 选择题

(1) 下面(　　)是文件传输协议。

A. IP　　B. TCP　　C. HTTP　　D. FTP

(2) TCP/IP 协议应用层中 FTP 协议与传输层进行交换数据是通过(　　)端口。

A. 80　　B. 110　　C. 21　　D. 28

(3) 访问经过 SSL 加密后的 FTP 站点要通过(　　)端口。

A. 80　　B. 23　　C. 8080　　D. 990

3. 思考题

(1) FTP 服务的工作原理是什么？

(2) 如何启用 FTP 服务器的 SSL 功能？



第6章　电子邮件服务器配置与管理

本章要点

- 电子邮件系统的工作原理和工作过程
- MDaemon 邮件服务器的安装、配置和管理

电子邮件服务是 Internet 最基本的服务，也是最重要的服务之一。据统计，Internet 上 30％以上的业务量是电子邮件，仅次于 WWW 服务。电子邮件服务是目前最常见、应用最广泛的一种互联网服务。通过电子邮件，可以与 Internet 上的任何人交换信息。电子邮件的快速、高效、方便以及价廉，越来越得到了广泛的应用，只要是上过网的网民就肯定用过电子邮件这种服务。目前，全球平均每天约有几千万份电子邮件在网上传输。

6.1　电子邮件服务概述

电子邮件的主要功能就是用来在 Internet 或 Intranet 上进行信息的传递和交流。与传统的邮政信件服务相比，电子邮件具有如下优势：

- 比人工邮件传递迅速，可达到的范围广，而且比较可靠。
- 不要求通信双方都在现场，不需要知道通信对象在网络中的具体位置。
- 可以实现一对多的邮件传送。
- 可以将文字、图像、语音等多种类型的信息集成在一个邮件中传送。

6.1.1　电子邮件服务的基本概念

电子邮件系统采用 Client/Server(客户端/服务器)工作模式，主要由邮件服务器、邮箱、电子邮件应用程序三个部分组成。

邮件服务器是邮件服务系统的核心，其主要功能如下：

- 接收用户送来的邮件，并根据目的地址将其传送到对方的邮件服务器。
- 接收从其他邮件服务器发来的邮件，并根据接收地址将其分发到用户邮箱中。

邮箱负责在邮件服务器中为每个合法用户开辟一个存储用户邮件的空间，其主要功能是为用户存储接收的电子邮件。邮箱是私有的，具有账号和密码属性，只有合法用户才能阅读其邮箱中的邮件。



电子邮件应用程序是邮件系统的客户端软件，其主要功能如下：

- 创建和发送邮件。
- 接收、阅读和管理邮件。
- 附加功能，如通讯簿管理、收件箱助理及账号管理等。

电子邮件地址的一般形式是 username@mail_server_domain_name，其中 mail_server_domain_name 代表邮件服务器的域名，username 代表服务器上的用户邮箱名。发送方的邮件服务器软件在发送邮件时，根据 mail_server_domain_name 来确定要连接的接收方邮件服务器，而接收方邮件服务器则使用 username 来选择对应的邮箱将收到的邮件存储起来。邮件地址具有唯一性，即邮件服务器域名在整个电子邮件系统中是唯一的，并且用户邮箱名在这台邮件服务器上也是唯一的。

6.1.2　电子邮件系统的工作原理

1. 电子邮件系统的工作机制

通常情况下，一封电子邮件的发送需要经过邮件用户代理（Mail User Agent，MUA）、邮件传送代理（Mail Transfer Agent，MTA）和邮件转发代理（Mail Delivery Agent，MDA）三个程序的参与。

MUA 的主要作用是将用户的邮件发送到邮件主机上或者将用户的邮件从邮件主机上接收下来。MUA 接收用户输入的各种指令，将用户的邮件传送至 MTA 或者通过 POP、IMAP 将信件从 MTA 服务器下载到本机上。其典型代表包括微软的 Outlook Express、腾讯的 Foxmail、Mozilla 的 Thunderbird（雷鸟）等邮件客户程序。

MTA 的主要作用是监视 MUA 的请求，根据电子邮件的目标地址找出对应的邮件服务器，将信件在服务器之间传输并且将接收到的邮件缓冲或者提交给 MDA。实际上，现在的 MTA 一般就是指邮件服务器，其典型代表包括 Windows 下的 Exchange、Imail Server、MDaemon 和 Linux/UNIX 下的 Sendmail、Qmail、Postfix、Exim 等。虽然从严格意义上说，MTA 只是具备 SMTP 的主机，但实际上现在的 MTA 基本包括了邮件发送、接收、转发三个方面的功能。

MDA 的作用是分析 MTA 处理的邮件中的表头或者其他数据，从而决定这封邮件的去向。另外，MDA 还具有邮件过滤（ filtering ）等功能。其典型代表包括 procmail 等。

当用户发送一封电子邮件时，并不能直接将信件发送到对方邮件地址指定的服务器上，而是必须首先试图去寻找一个 MTA，把邮件提交给它；MTA 得到了邮件后，首先将它保存在自身的缓冲队列中，然后，根据邮件的目标地址，MTA 程序查询到应对这个目标地址负责的 MTA 服务器，并且通过网络将邮件传送给它。对方的 MTA 服务器接收到邮件之后，将其缓冲存储在本地，直到电子邮件的接收者查看自己的电子信箱。显然，邮件传输是从服务器到服务器的，而且每个用户必须拥有服务器上存储信息的空间（即邮箱空间）才能接受邮件，发送邮件则不受这个限制。而 MDA 则从 MTA 取得信件传送至最终用户的邮箱。显然，最终用户只能看到用户邮件转发代理。



2. 电子邮件系统中的通信协议

电子邮件客户端和服务器端种类繁多,那么它们之间是按照什么规则来通信的呢?是协议,即电子邮件协议,如图6-1所示。

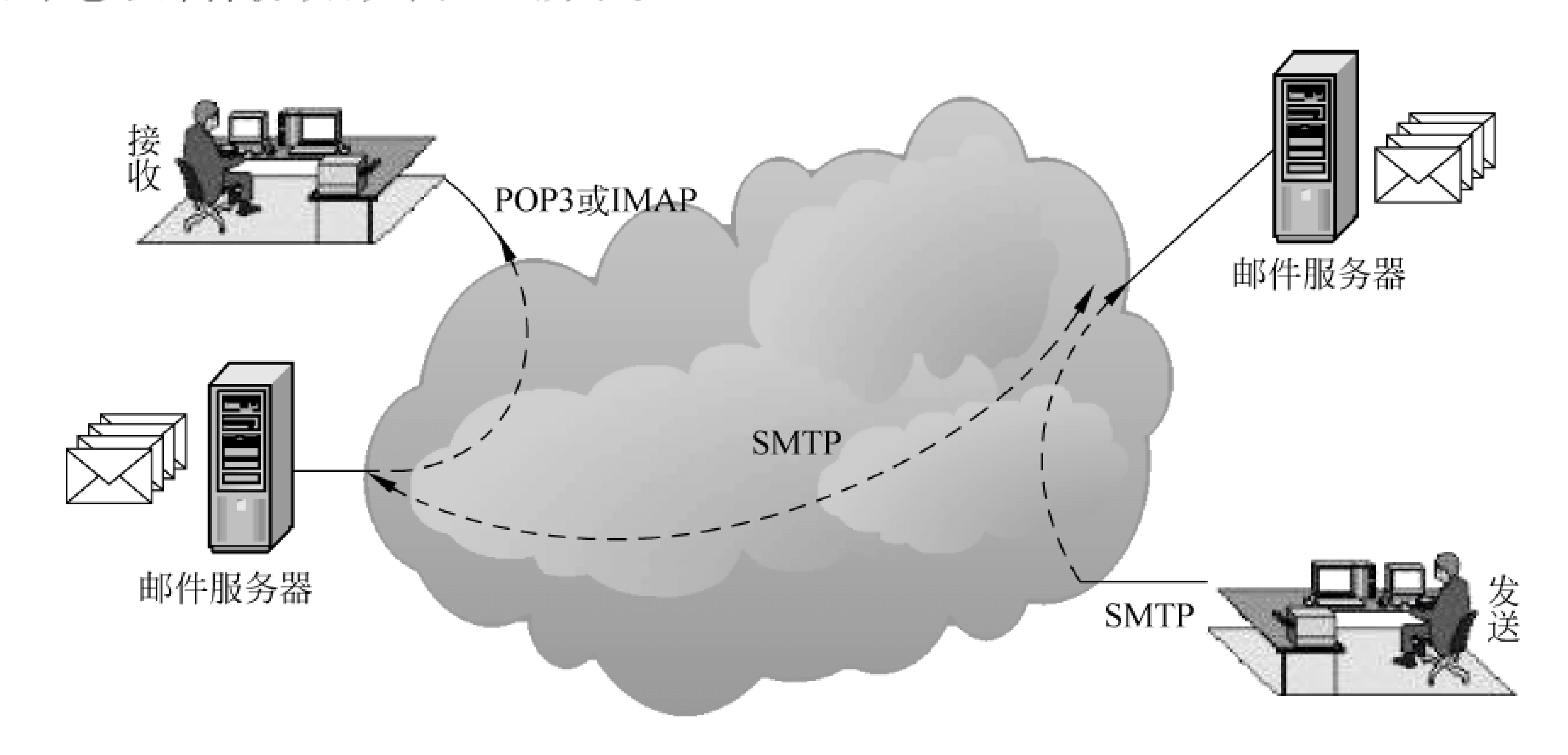


图6-1 电子邮件系统中的通信协议

从图6-1中可以看出,邮件客户端和邮件服务器通过POP3或IMAP收取邮件,通过SMTP发送和传输邮件内容,实现邮件信息交换。SMTP通过MUA和MTA等程序实现邮件的传输。

发送方编辑完毕的电子邮件发送给当地的邮件服务器,邮件服务器收到客户送来的邮件,根据收件人的邮件地址发送到对方的邮件服务器中。对方的邮件服务器接收到其他邮件服务器发来的邮件,并根据邮件地址分发到相应的电子邮箱中,这样接收方可通过电子邮箱来读取邮件,并对它们进行相关地处理。

(1) SMTP。SMTP的全称是Simple Mail Transfer Protocol,即简单邮件传输协议,目标是向用户提供高效、可靠的邮件传输。SMTP的一个重要特点是它能够在传送中接力传送邮件,即邮件可以通过不同网络上的主机接力式传送。它工作在两种情况下:一是电子邮件从客户端传输到服务器;二是从某一个服务器传输到另一个服务器。SMTP是请求/响应协议,它监听25号端口,用于接收用户的邮件请求,并与远端邮件服务器建立SMTP连接。

(2) POP3。POP的全称是Post Office Protocol,即邮局协议,用于接收电子邮件,它使用TCP的110端口。现在常用的是第3版,所以简称POP3。

POP3采用Client/Server工作模式,当客户端需要服务时,客户端的软件(如Outlook Express或Foxmail等)将与POP3服务器建立TCP连接,此后要经过POP3协议的三种工作状态。首先是认证过程,确认客户端提供的用户名和密码,在认证通过后便转入处理状态;在此状态下用户可收取自己的邮件或删除邮件,在完成相应的操作后客户端便发出退出命令;此后便进入更新状态,将做删除标记的邮件从服务器端删除。至此,整个接收过程完成。

(3) IMAP4。IMAP的全称是Internet Message Access Protocol。即Internet消息访问协议。顾名思义,主要提供的是通过Internet获取信息的一种协议。IMAP像POP一样

提供了方便的邮件下载服务，让用户能进行离线阅读。但 IMAP 能完成的却远远不只这些，IMAP 提供的摘要浏览功能，可以让用户在阅读完所有的邮件到达时间、主题、发件人、大小等信息后才做出是否下载的决定。IMAP4 是其第 4 版。

IMAP 本身是一种用于邮箱访问的协议，使用 IMAP 协议可以在邮件客户端管理服务器上的邮箱。它与 POP3 不同，邮件是保留在服务器上而不是下载到本地，在这一点上 IMAP 是与 Web Mail 相似的。但 IMAP 有比 Web Mail 更好的地方，即它比 Web Mail 更高效和安全，可以离线阅读等。

（4）Web Mail。说到电子邮件，就不能不提到 Web Mail 这种目前最热门的邮件管理方式，163、Gmail、Hotmail 等就是这种电子邮件的代表。Web Mail 并不是一种协议，它只不过是服务器上专门针对邮件程序安装的 Web 支持插件，让客户端通过浏览器即可查收、阅读和发送邮件。由于是通过浏览器来执行上述操作的，所以使用起来更方便。

6.1.3　电子邮件系统的工作过程

1. 发送邮件

电子邮件的发送与日常生活中的邮政服务类似，具体的六个步骤如图 6-2 所示。

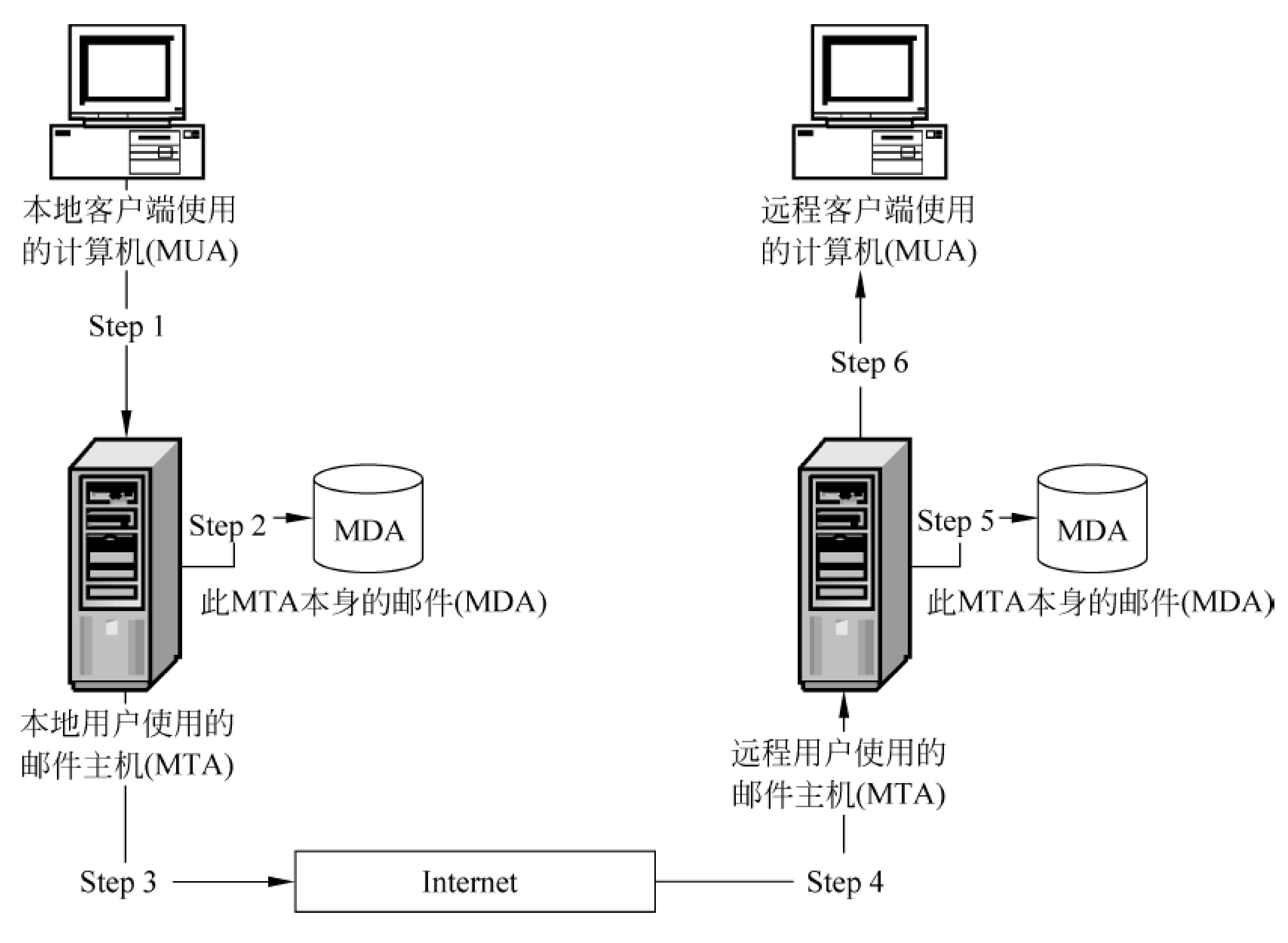


图 6-2　电子邮件从邮件主机发送邮件示意图

（1）发件人利用 MUA（如 Outlook Express 等）寄信到 MTA。

写信时通常会明确以下信息：

- 发件人即发送服务器，该服务器为第二步接收信件的 MTA。
- 收件人即接收服务器，一般以 username@mail_server_domain_name 的形式呈现，其中 mail_server_domain_name 代表邮件服务器的域名，而 username 代表服务器上的用户邮箱名。



此时利用 MUA 的功能在本地客户端使用的计算机上写好信后，按下 MUA 的【发送】按钮，MUA 就会按照发件人地址将信发送到其 MTA 上面。

（2）MTA 收到本服务器地址的信件，交由其 MDA 发送到该账号的邮箱中。如果在第一步所发送的信件中，收件人地址中的邮箱服务器就是 MTA 自己，此时 MTA 会将该信件交由其 MDA 去处理，将信件放置在相应收件人的信箱中。

（3）MTA 将邮件转发。如果在第一步所发送的信件中，收件人地址并不是 MTA 的内部账号，则 MTA 还要负责将这封邮件转发出去，直到到达最终地点。这就是 MTA 的转发(Relay)功能。

（4）远程 MTA 接收本地 MTA 所转发的邮件。远程的 MTA 会接收本地 MTA 所转发的邮件，并将邮件交给其 MDA 处理（第（5）步），此时信件会存放在远程 MTA 上，等待收件人登录读取或者下载到本地计算机。

（5）MTA 收到本服务器地址的信件，交由其 MDA 发送到该账号的邮箱中。

2．接收邮件

接收方的邮件服务器收到发信请求后，会接收邮件，然后将邮件保存到本地的用户邮箱中，等待用户通过 POP3、IMAP4 或者 Web 方式来收取。接收邮件的工作过程如图 6-3 所示。

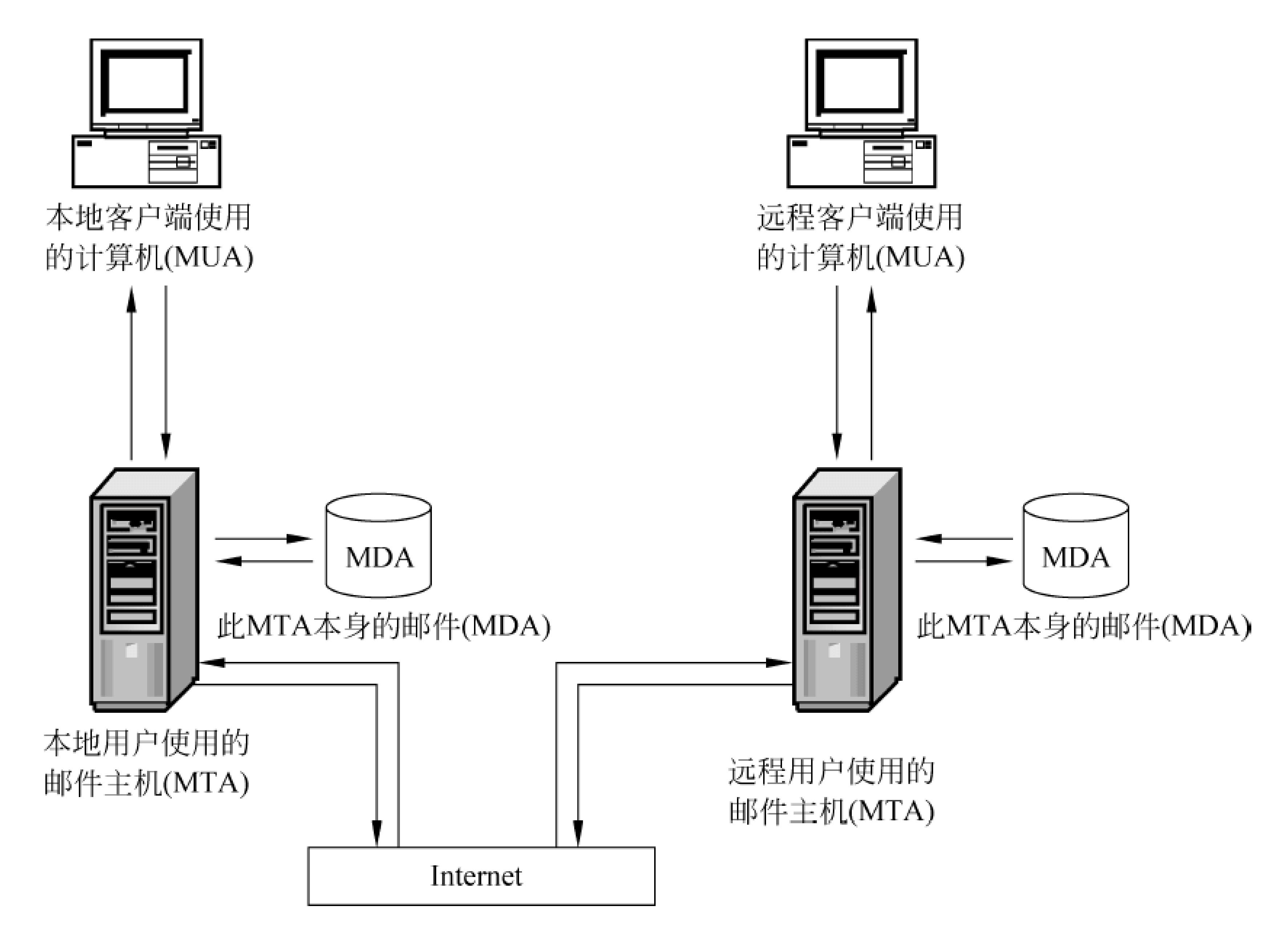


图 6-3　客户端接收邮件主机的电子邮件示意图

远程客户端使用的计算机直接连接到其 MTA，向 MTA 发送请求，要求查看自己的邮箱是否有信件。而 MTA 通过 MDA 检查后，如果有信件，就使用 POP3 或者 IMAP4 协议，让客户端通过 MUA 将邮件接收下来。同时，根据 MUA 的不同设置，MTA 会选择将该邮箱的邮件清除或者继续保留。通常 MUA 都是预置为清除 MTA 上的邮箱内容。



6.2　MDaemon 邮件服务器的安装

MDaemon 邮件服务器软件是美国 Alt-N 公司出品的一款优秀的邮件服务器软件。其大量的高级反垃圾邮件防范措施、设计良好的界面以及合理的价格，使其在众多的竞争产品中脱颖而出，成为世界上最流行的邮件服务器软件之一。MDaemon 定位于任何个人用户的邮件需求和要求，包括一套强大的整合工具，以便于管理账户和邮件格式。MDaemon 提供了一套可扩展的 SMTP、POP3 和 IMAP4 邮件服务器，其中包括 LDAP 支持、AD 支持、整合的基于浏览器的邮件客户端、内容过滤器、垃圾邮件拦截器、广泛的安全性能等，特别适用于那些既需要在局域网中互相发送电子邮件，又需要同 Internet 互发邮件的用户。

本章以 MDaemon v10.0 版本邮件服务器软件为例进行讲解，该版本同样是一款基于标准 SMTP/POP3/IMAP4 协议并提供全部邮件服务功能的邮件服务器软件。它不仅支持 Windows XP/2003/2000 的操作系统，还支持 Windows、Vista/2008 等操作系统。读者可以从 Alt-N 公司官方网站 http://www.altn.com 或者中文网站 http://www.altn.cn 上下载试用 MDaemon 邮件服务器软件 30 天试用版本，体验 MDaemon 的强大功能。

在 Windows Server 2003 环境下，MDaemon v10.0 的安装步骤如下。

6.2.1　安装准备工作

1. 查看服务器硬件配置

服务器硬件配置要求取决于使用 MDaemon 的用户数以及用户的邮件通信量。在许多情况下，完全可以使用现有的硬件和操作系统来运行 MDaemon，避免了额外的硬件投入。

最低要求如下：

- Pentium Ⅲ 500 MHz 以上处理器；
- 1GB 以上内存(推荐 2 GB)；
- 60MB 硬盘空间，存储邮件会产生额外的空间需求；
- Microsoft Windows XP/NT/2000/2003 操作系统；
- Winsock 2；
- Internet Explorer 5.0 以上版本；
- Ethernet 网卡；
- 安装 TCP/IP 网络协议；
- 互联网或局域网通信能力。

2. 调整操作系统服务和设置

(1) 在系统服务中关闭 Windows 自身的 SMTP 服务和 POP3 服务。如果系统中已经架设了利用 Windows 2003 自带 POP3/SMTP 服务或者其他第三方软件实现的邮件服务器，则需要首先关闭这些服务，以便释放 25 端口供 MDaemon 使用。具体操作步骤如下：

① 在 Windows 2003 系统中依次选择【开始】→【控制面板】→【管理工具】→【服务】命



令，在打开的【服务(本地)】窗口中选择 Simple Mail Transfer Protocol(SMTP)服务，如图 6-4 所示，并将该服务启动类型设置为“禁用”。

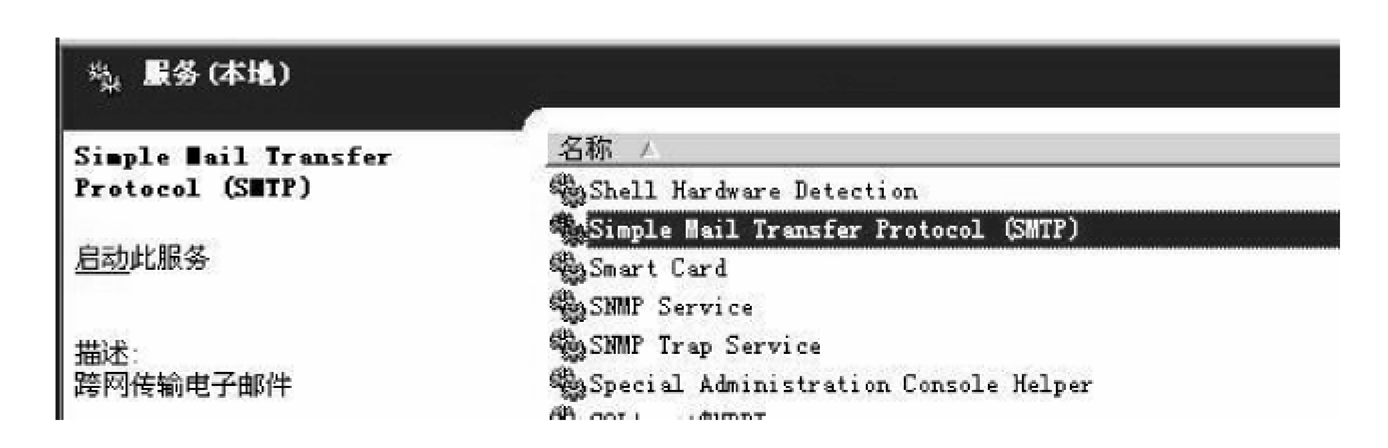


图 6-4 关闭 SMTP 服务

② 在【服务(本地)】窗口中选择 Microsoft POP3 Service 服务，如图 6-5 所示，并将该服务启动类型设置为“禁用”。



图 6-5 关闭 POP3 服务

③ 卸载其他邮件服务器软件，直到 25 端口无程序占用。

④ 在 Windows 2003 系统中依次选择【开始】→【控制面板】→【添加/删除软件】命令，卸载其他邮件服务器软件。

⑤ 在 Windows 2003 系统中依次选择【开始】→【运行】命令，在弹出的【运行】对话框中输入 cmd 后按 Enter 键，会弹出【命令提示符】对话框，如图 6-6 所示。输入 telnet 127.0.0.1 25 测试服务器本机 25 端口是否有程序占用。反复测试，直到出现提示字样。



图 6-6 测试服务器 25 端口是否被占用

(2) 关闭和调整 Windows 自身网络防火墙的设置。在安装 MDaemon 服务器之前，需要首先关闭 Windows 系统自身的防火墙。具体操作步骤如下：

① 在 Windows 2003 系统中依次选择【开始】→【设置】→【网络连接】命令，在弹出的【网络连接】对话框中双击使用中的网卡，会弹出【网络连接 状态】对话框。



② 单击【属性】按钮，会弹出【网络连接 属性】对话框。

③ 选择【高级】选项卡，单击【Windows 防火墙】选项区域中的【设置】按钮，会弹出【Windows 防火墙】对话框。

④ 选中【关闭】单选按钮，关闭防火墙。

⑤ 如果必须开启防火墙，则需要在防火墙中开启【SMTP 服务】(25 端口)和【POP 服务】(110 端口)等端口。

(3) 如果操作系统是 Windows 2003 SP1 版本，则还需要做如下设置：

① 依次选择【开始】→【控制面板】命令，会弹出【控制面板】窗口，如图 6-7 所示。



图 6-7　【控制面板】窗口

② 双击【系统】图标，会弹出【系统属性】对话框，如图 6-8 所示。

③ 选择【高级】选项卡，单击【性能】选项区域中的【设置】按钮，会弹出【性能选项】对话框，如图 6-9 所示。

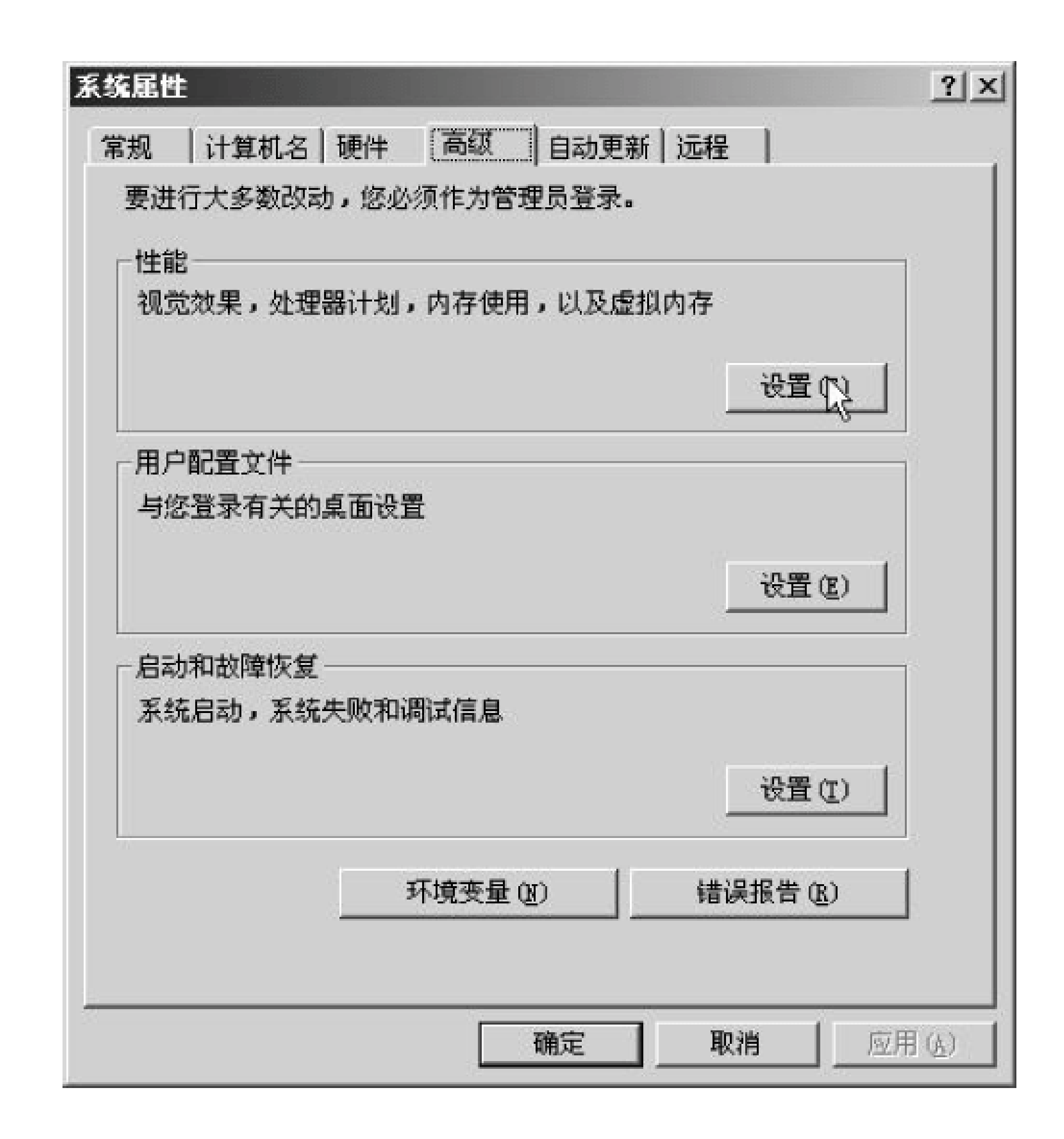


图 6-8　【系统属性】对话框

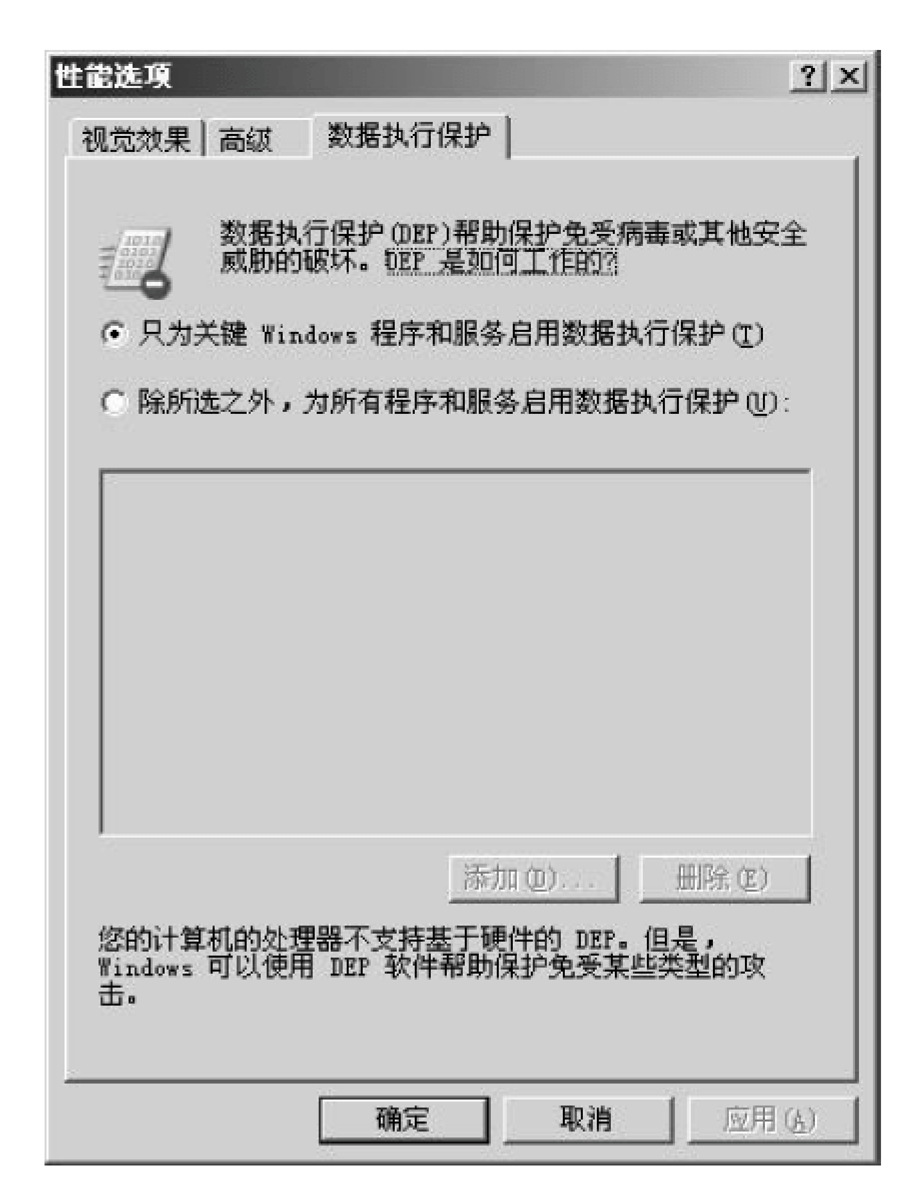


图 6-9　【性能选项】对话框



④ 选择【数据执行保护】选项卡，选中【只为关键 Windows 程序和服务启用数据执行保护】单选按钮。

6.2.2 MDaemon 邮件服务器的安装过程

MDaemon 邮件服务器的安装步骤如下：

(1) 双击，运行 MDaemon 安装包 md1000_zh.exe 文件，出现安装欢迎界面，如图 6-10 所示。单击【下一步】按钮。



图 6-10 安装欢迎界面

(2) 出现许可协议界面，如图 6-11 所示。单击【我同意】按钮。



图 6-11 许可协议界面

(3) 出现选择安装目录界面，如图 6-12 所示。MDaemon 的安装支持全新和升级方式，并且对所在分区和目录没有特殊要求。单击【下一步】按钮。

(4) 出现注册信息界面，如图 6-13 所示。按要求输入许可名、公司或销售商和注册码，然后单击【下一步】按钮。也可以什么也不填，系统将自动产生一个 MDaemon Pro 无限用户 30 天试用的注册码。在 30 天试用期间，可以随时输入正版序列号使软件成为正式版，而无须重新安装。

(5) 出现准备安装界面，如图 6-14 所示。单击【下一步】按钮，开始安装。







图 6-12　选择安装目录界面



图 6-13　注册信息界面



图 6-14　准备安装界面

(6) 出现安装界面，如图 6-15 所示。此时应等待安装程序复制文件到硬盘。

(7) 安装完以后，出现域名设置界面。此时系统默认产生一个名为 company.mail 的域名，请务必将其改成自己申请的域名，此处改为 test.com，如图 6-16 所示。系统

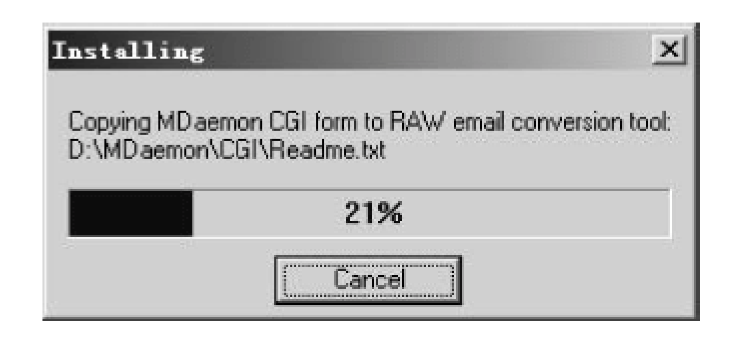


图 6-15　安装界面





将此域名作为 MDaemon 的主域名。单击【下一步】按钮。



图 6-16　域名设置界面

(8) 出现第一个账号设置界面,如图 6-17 所示。此处应根据屏幕提示设置管理员账号名称、邮箱名称以及密码等信息,其中密码位数不小于六位。该账号应具有全局管理员的权限,这里 MDaemon 不会要求强密码。当然,如果不需要 Web 方式管理,也可以不将此账号默认为全局管理员。但为了方便管理,不建议这样设置。设置完成,单击【下一步】按钮。



图 6-17　管理员账号设置界面

(9) 出现 DNS 设置界面,如图 6-18 所示。在此处要求定义 DNS 服务器,如果选中【使用 Windows 的 DNS 设置】复选框,则 MDaemon 自动启用系统网络 TCP/IP 设置中的 DNS 配置。如果取消选中【使用 Windows 的 DNS 设置】复选框,则必须手动输入 DNS 服务器地址。强烈建议这里选中【使用 Windows 的 DNS 设置】复选框。单击【下一步】按钮。

(10) 出现服务器设置界面,如图 6-19 所示。此处建议把 MDaemon 作为系统服务来运行,这样无须用户登录系统,MDaemon 就可以在服务器启动后在后台自动启动。单击【下一步】按钮。

(11) 出现安装完成界面,如图 6-20 所示。选中【启动 MDaemon】复选框,并单击【完成】按钮,即可完成 MDaemon 的整个安装过程。

如果在安装过程中没有填写序列号,那么 MDaemon 在第一次启动时,会分配一个 30





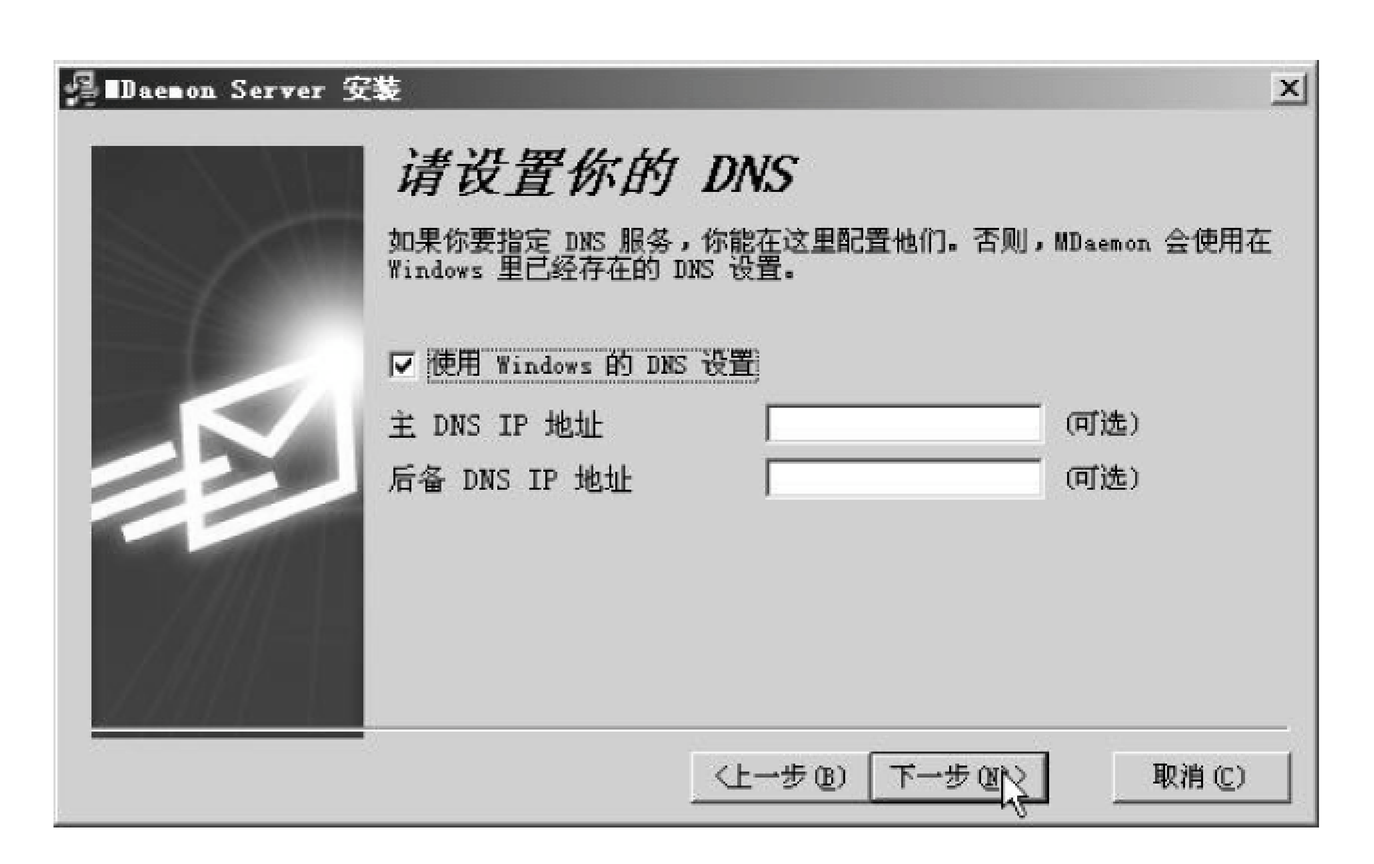


图 6-18　DNS 设置界面



图 6-19　服务器设置界面



图 6-20　安装完成界面

天使用期限的无限制序列号，所以这里会弹出一个友情提示，如图 6-21 所示。此时不必记录该序列号，因为它在试用过程中没有任何作用。单击【确定】按钮。

MDaemon 开始启动并进行一系列初始化配置，启动完成后的程序主界面如图 6-22 所示。





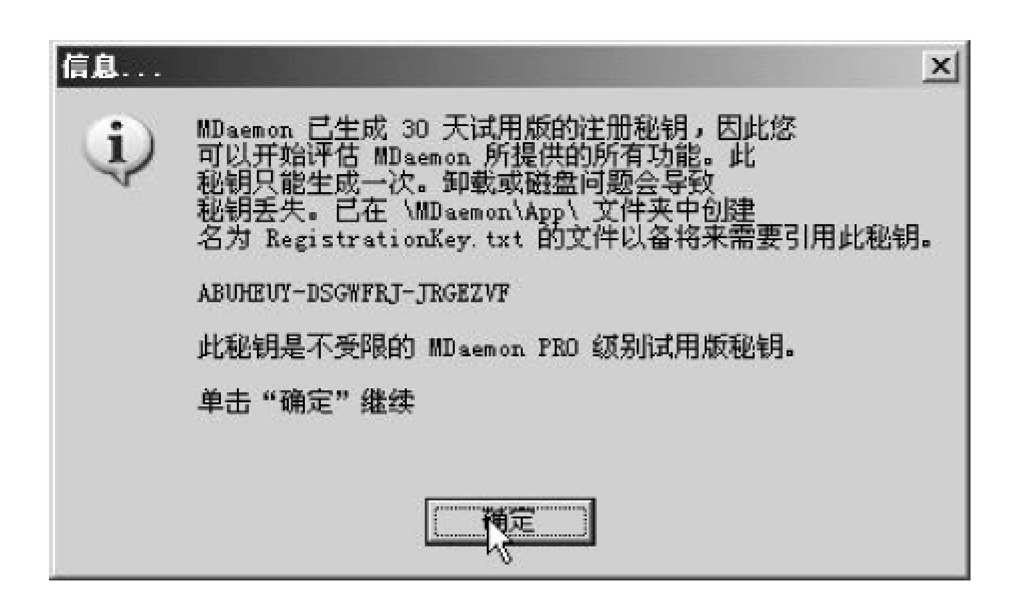


图 6-21 试用序列号界面



图 6-22 程序主界面

6.2.3 MDaemon 插件的安装

除基本的邮件服务器功能外，MDaemon 还具有大量的插件来进行功能扩展。常见的插件包括如下几个。

(1) 内嵌防病毒插件 SecurityPlus。SecurityPlus for MDaemon 是 Alt-N 公司开发的一个 E-mail 病毒检查器插件。SecurityPlus for MDaemon 在 E-mail 到达邮件服务器时进行病毒扫描。SecurityPlus 同时扫描邮件的正文和附件，一旦发现问题，MDaemon 邮件服务器就会拒绝接收该邮件。有时候，MDaemon 会在收取这类邮件后将其隔离，尝试清除其中的病毒或者直接将其删除。而后，可以设置 SecurityPlus 是否通知相应发件人或收件人。

(2) 内置群组共享工具 Outlook Connector。Alt-N 开发出 Outlook Connector 来为中小应用程序提供经济和安全的群组共享功能。Outlook Connector 实时将用户与 Microsoft Outlook 的协作功能连接，使用 MDaemon 作为群件服务器。

(3) 传真服务器 RelayFax。RelayFax 是一个具有 OCR 和 TWAIN 功能的强大的传真服务器。它能把调制解调器变成传真机。通过强大且灵活的用户定义规则，收发的传真将以邮件形式传输给用户。此外，RelayFax 还能包含一系列的标准，如 OCR、Caller-ID 或传



真设备。RelayFax 是一个高效而又经济的传真解决方案。

（4）Web 邮件客户端 WorldClient。WorldClient 提供了一套完整的 Web Mail 邮件服务，使用户无论在办公室、家庭、网吧等地点都能随处随时保持联络。

（5）邮件安全网关 SecurityGateway。SecurityGateway 提供了简单易用的功能来分析、管理和报告位于 Microsoft Exchange Server 或任何 SMTP 邮件服务器上的入站与出站邮件通信量模式。

在 MDaemon 10.0 版本中，WorldClient 和 WebAdmin 插件是默认安装的，其他插件则需要根据用户要求单独安装。这里以 SecurityPlus 内嵌防病毒插件的安装为例进行说明。具体操作步骤如下：

（1）双击运行从 Alt-N 网站上下载的安装包 av402_zh.exe 文件，出现安全警告界面，如图 6-23 所示。单击【运行】按钮。

（2）出现安装欢迎界面，如图 6-24 所示。单击【下一步】按钮。

（3）出现许可协议界面，如图 6-25 所示。单击【我同意】按钮。

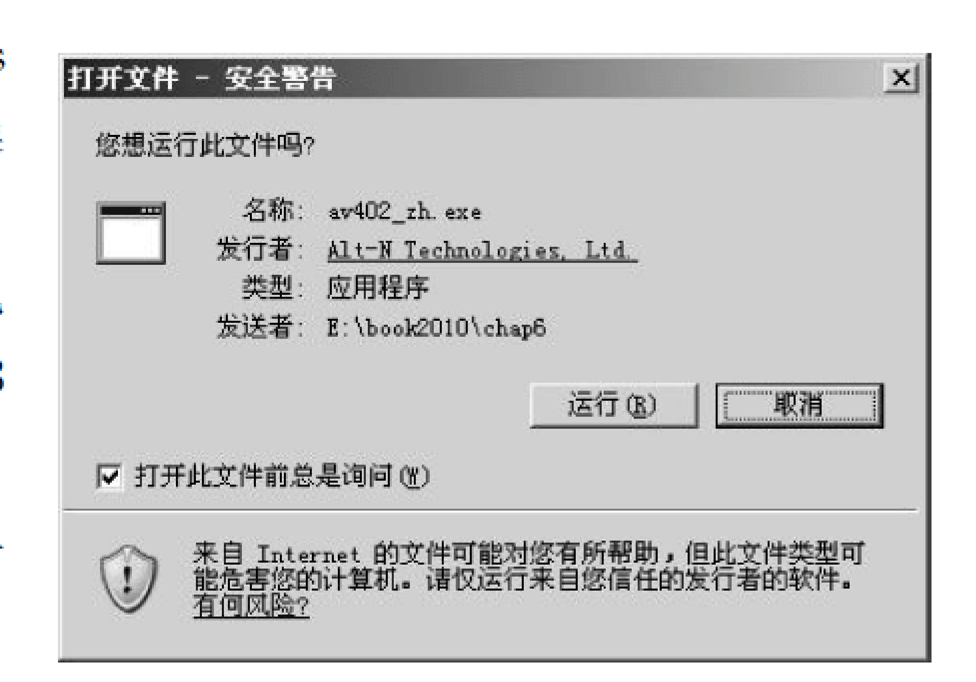


图 6-23 安全警告界面



图 6-24 安装欢迎界面



图 6-25 许可协议界面



(4) 出现选择目标目录界面,如图 6-26 所示。在这里选择默认路径安装,因此直接单击【下一步】按钮。



图 6-26　选择目标目录界面

(5) 出现准备就绪界面,如图 6-27 所示。单击【下一步】按钮,开始安装。



图 6-27　准备就绪界面

(6) 如果在开启 MDaemon 主程序的情况下开始安装 AV 插件,此时会出现警告界面,如图 6-28 所示。单击【继续】按钮,会首先终止 MDaemon 邮件服务器的运行,再开始安装 AV 插件。

(7) 出现安装界面,如图 6-29 所示。此时应等待安装程序复制文件到硬盘,在此过程中也可以随时单击 Cancel 按钮来取消安装。

(8) 安装完成以后,出现安装完成界面,如图 6-30 所示。选中【启动带有 SecurityPlus 的 MDaemon】复选框,并单击【完成】按钮,将重新启动 MDaemon 邮件服务器以启用 AV 防护功能。





图 6-28　警告界面

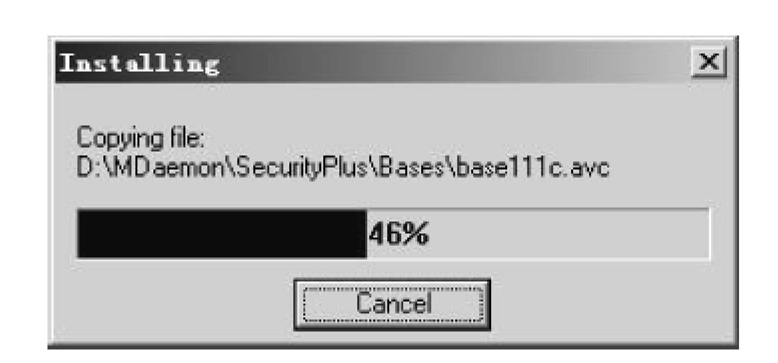


图 6-29　安装界面



图 6-30　安装完成界面

(9) 安装完毕并重新启动 MDaemon 后，会出现病毒库升级界面，如图 6-31 所示。此时自动启动病毒库升级程序进行升级。因为版本的缘故，有时需要更新的数据可能会很大，这时应耐心等待其结束。升级结束后 AV 插件安装正式完成，系统自动进入 MDaemon 的程序主界面，如图 6-22 所示。



图 6-31　病毒库升级界面



6.3 MDaemon 邮件服务器的配置与管理

从图 6-22 中可以看出，MDaemon 的主图形用户界面（GUI）提供了关于 MDaemon 的资源、统计、活动会话以及等待处理的队列邮件的重要信息，还包括可以方便地激活或关闭 MDaemon 各种服务器的选项。GUI 的标签面板可以保持最新的状态以查看服务及输入/输出连接的运行情况等。除了常见的菜单栏、工具栏、状态栏以外，其 GUI 主要由左、右两个窗格组成，分别是统计窗口、事件跟踪与记录日志窗口。

1. 统计窗口

默认情况下，统计窗口在 MDaemon 主界面的左窗格中。该窗口包含三个部分：统计、队列和服务器。

统计部分包含 MDaemon 收发邮件数量的统计以及从启用开始初始化的邮件会话数量的统计。这个部分会显示有多少账户已经存在以及还可以创建多少账户。统计部分提供两种右键快捷菜单：一个用于账户项目；另一个用于邮件计数器统计项目。通过账户快捷菜单，可以方便地创建、编辑以及删除账户。通过邮件计数器统计快捷菜单，则可以清除邮件计数。

队列部分包含一个用于每个邮件队列的条目和每一个队列包含的邮件数量。

服务器部分包括了用于 MDaemon 服务器的每个服务条目，而且这些条目都列出了服务的当前状态：活动或者不活动。每个服务条目对应于一个当前正在使用的端口与 IP 地址。快捷菜单提供了在每个服务的活动和非活动状态间切换的控制。

2. 事件跟踪与记录日志窗口

主界面上默认的右边窗格包含一组标签，显示 MDaemon 的各种服务器与资源的当前活动和状态，并且这些信息会持续更新以反映当前服务器的最新状态。一旦有活动完成，每个活动会话与服务器活动就会被记录到正确的标签中。如果选择记录那些活动，显示在标签上的信息还会被镜像到日志目录里的日志文件中。

6.3.1 基本配置与管理

虽然 MDaemon 的主图形用户界面（GUI）很专业，所提供的选择和设置项目非常多，但是实际上真正需要设置的选项并不是很多，大部分都采用默认值即可。其基本配置与管理功能主要是在【设置】菜单里完成的，如图 6-32 所示。



图 6-32 【设置】菜单

- 默认域/服务器：用来配置系统默认域和其他服务器选项，可以指定默认域的名称及其 IP 地址，配置服务器和邮件协议，设置 MDaemon 监控 SMTP、POP3 和 IMAP4 事件的端口，指定 DNS 服务器 IP 地址，指定收发邮件的最大并发会话线程数以及超时设置等。



- 额外域：MDaemon 服务器全面支持多域(仅限 MDaemon 专业版)，支持多重绑定(多个不同的域共享一个 IP)。可以在这里指定任意的额外域以及其 IP 地址。
- Web 及 SyncML 服务：可以指定 Web Mail 设置以及对服务器进行远程管理的一些设置。
- 事件调度：MDaemon 的事件调度程序，可以使用计数器定期处理邮件，或使用邮件调度功能来安排邮件投递和收集的确切时间，设置在非预订时间触发邮件处理的条件等。此外，还可以指定防病毒模块的更新设置。
- 首选项：设置 MDaemon 服务器的运行首选项以及在 Windows 系统中的服务方式。

这里仅以【设置】菜单下面的【Web 及 SyncML 服务】命令为例进行详细说明。

(1) 打开【设置】菜单，如图 6-32 所示。

(2) 选择【Web 及 SyncML 服务】命令，会弹出【WorldClient(Web 邮件)】对话框。在该对话框可以启用 WorldClient 服务器并配置各种与 WorldClient 相关的设置，如指定其运行端口等，还可以控制许多全局或者域的特定设置，如使用的默认语言和主题、用户是否可以创建账户、邮件列表的默认分页、是否启用 ComAgent 支持、是否允许及记录即时消息、配置对 SSL 与证书的支持、RelayFax 集成等。该对话框由左、右两个窗格组成，在左侧窗格选择相应选项，就会在右侧窗格显示相应信息。

在左侧窗格选择【Web 服务器】选项，如图 6-33 所示。

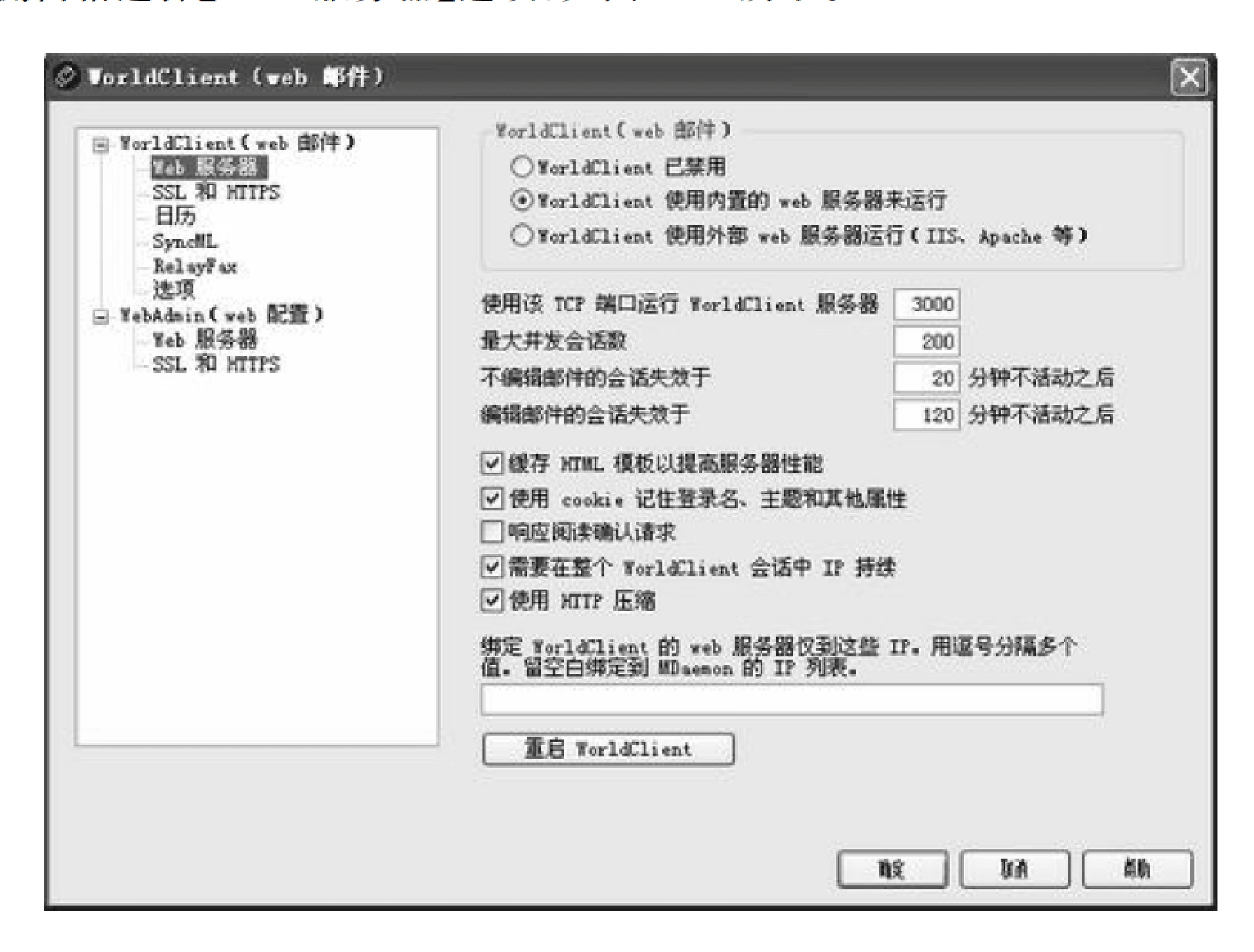


图 6-33　WorldClient 的【Web 服务器】选项

此时在该对话框右侧可以设置邮件服务器的一些最基本参数：

- WorldClient 已禁用。选择此单选按钮来禁用 WorldClient。另外，还可以从【文件】菜单或从 MDaemon 主界面上统计窗口的【服务器】部分切换 WorldClient 的活动/非活动状态。



- WorldClient 使用内置的 Web 服务器来运行。选择此单选按钮以使用 MDaemon 的内置 Web 服务器来运行 WorldClient。这也是默认的配置。
- WorldClient 使用外部 Web 服务器运行(IIS、Apache 等)。如果希望 WorldClient 运行在 IIS 或其他 Web 服务器之下而不使用 MDaemon 的内置 Web 服务器,则选择此单选按钮。
- 使用该 TCP 端口运行 WorldClient 服务器。在该文本框中指定访问 WorldClient 所使用的端口号。系统默认值为 3000,即用户可通过 http://mail_server_ip_address:3000(其中 mail_server_ip_address 指邮件服务器的域名)对 WorldClient 进行访问。当然,该端口号可以自行修改为任何还没有被系统占用的端口。
- 最大并发会话数。在该文本框中指定可以同时连接到 WorldClient 的最大会话数。
- 不编辑邮件的会话失效于。在该文本框中指定闲置连接超时的时间。例如,当设置为 20 时,如果客户端在 20min 内未执行任何邮件操作任务,那么系统即置该连接为超时。用户再连接该服务器时,需要重新验证用户名和密码。
- 编辑邮件的会话失效于。在该文本框中指定连接超时的时间。例如,当设置为 120 时,如果用户对邮件服务器连接操作超过了 120min,则系统也认为为超时,将强行切断该连接,以要求该用户重新登录。该设置既有助于杜绝用户发送超大容量的附件,又有助于禁止用户发送大量的垃圾邮件。
- 缓存 HTML 模板以提高服务器性能。选中该复选框,将把 HTML 模板装载到 Cache 中以提高 Web 服务的性能。
- 使用 cookie 记住登录名、主题和其他属性:选中该复选框,系统将使用 cookie 来存储用户名、用户自定义风格以及其他数据。系统默认使用了该选项,但是如果用户经常在公众场所如网吧上网,那么建议取消该项以增加安全性。
- 需要在整个 WorldClient 会话中 IP 持续。选中该复选框,要求在同一 IP 地址上独立完成同一 WorldClient 进程。这一点也是从安全角度考虑,所以建议把此选项也选中。
- 绑定 WorldClient 的 Web 服务器仅到这些 IP。在该文本框中输入 IP 地址信息,以便将 WorldClient 绑定到该地址。如果拥有多个 IP 地址、设置了虚拟主机,并且希望用户通过不同的 IP 地址来访问相同的一个 WorldClient 服务,那么可以将所有希望绑定的 IP 地址都填入该文件框,并且多个 IP 地址之间用逗号来隔开。如果留空,则表明只是希望使用 MDaemon 本身的 IP 地址。
- 重启 WorldClient。单击该按钮,将重启 WorldClient。通常情况下,都是在修改了 WorldClient 端口或者其他选项后才使用它。

(3) 在左侧窗格选择【选项】选项,如图 6-34 所示。

该对话框右侧的各具体参数设置如下:

- 选择域。在该下拉列表中选择 WorldClient 所使用的域名。如果只使用了一个域名,则选择 Default。
- 语言。在该下拉列表中选择语言,如中文选择 zh(Chinese)。系统本身支持中文的 WorldClient 界面,对英语基础不是很好的读者来说,这无疑是一个非常好的设置。



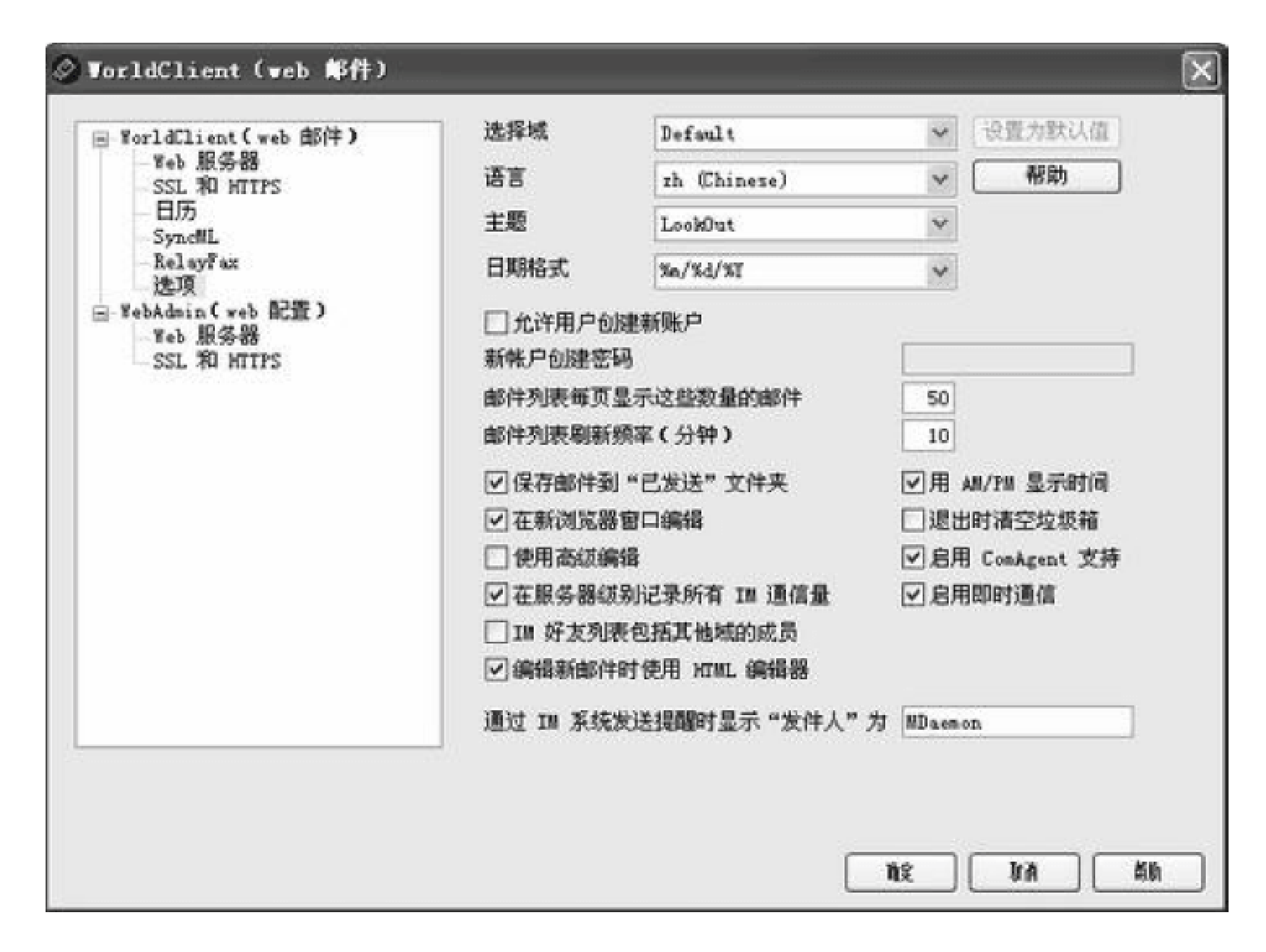


图 6-34　WorldClient 的【选项】设置

- 主题。在该下拉列表中选择页面风格。WorldClient 自带了几种风格模板,用户可以在这里设置系统默认的模板。
- 日期格式。在该下拉列表中选择日期格式。
- 允许用户创建新账户。选中该复选框,将允许用户自己建立新账户。这就是 MDaemon 非常体贴用户的一个设计。由于允许用户自动申请信箱,这就免去了管理员手动添加用户的苦恼。
- 新账户创建密码。在该文本框中输入新账户的默认密码。
- 邮件列表每页显示这些数量的邮件。在该文本框中输入每页默认显示的邮件数量。
- 邮件列表刷新频率(分钟)。在该文本框中输入邮件信箱的默认刷新频率。
- 保存邮件到“已发送”文件夹。选中该复选框,将在发送邮件的同时在发送文件夹中保存一个副本。该选项可能会大量占用磁盘空间,但对于查找邮件内容却非常有用。
- 在新浏览器窗口编辑。选中该复选框,将开启新窗口以编辑邮件。
- 使用高级编辑。选中该复选框,将使用高级编辑模式。
- 启用 ComAgent 支持。选中该复选框,将启用代理支持。
- 启用即时通信。选中该复选框,将直接发送邮件。
- 以服务器级别记录所有 IM 通信量。选中该复选框,将记录所有传送记录到日志文件中。
- IM 好友列表包括其他域的成员。选中该复选框,IM 的好友清单可包含其他域名用户。
- 用 AM/PM 显示时间。选中该复选框,使用 AM/PM 格式显示时间。
- 退出时清空垃圾箱。选中该复选框,在退出时清空本人邮箱中的回收站。

(4) 单击【确定】按钮,以保存对设置所做的修改。



6.3.2 安全配置与管理

MDaemon 配备有一套完善的安全功能和控件。其安全配置与管理功能主要是在【安全】菜单里完成的，如图 6-35 所示。

其中：

（1）AntiVirus 命令只有在安装了 SecurityPlus for MDaemon 插件后才可用，它可配置以下安全功能：

SecurityPlus for MDaemon 防病毒插件为 MDaemon 用户提供最高级别的集成保护，可以阻止以电子邮件为载体的计算机病毒。它会自动捕获、隔离、修复和/或删除任何被发现含有病毒的电子邮件。

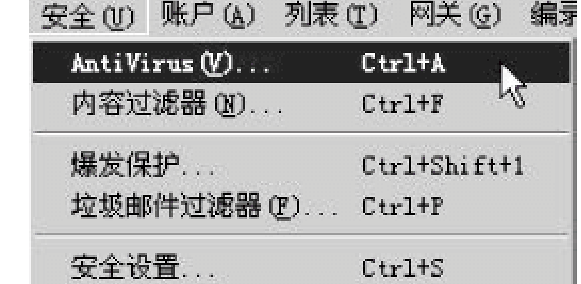


图 6-35 【安全】菜单

（2）【内容过滤器】：内容过滤器是一个高度灵活且完全多进程的内容过滤系统，它能基于入站和出站邮件的内容定制服务器的行为。该命令可配置以下安全功能：

用户可以插入和删除邮件报头，添加邮件页脚，删除附件，将副本路由到其他用户，向某人发送即时消息，运行其他程序等。

（3）【爆发保护】：爆发保护是一种革命性的实时反垃圾邮件、反病毒和反网络钓鱼（利用网络骗取用户信息）的技术。该命令可配置以下安全功能：

能够在爆发发生后的数分钟内前瞻性地自动保护 MDaemon 邮件架构。爆发保护是完全的内容不可知保护，不需要任何启发式规则、内容过滤或特征更新。

（4）【垃圾邮件过滤器】命令可配置以下安全功能：

- 垃圾邮件过滤器。使用垃圾邮件过滤技术，以启发式方法来检查电子邮件，从而计算一个“得分”。该分数用来确定邮件为垃圾邮件的可能性。基于该确定结果，服务器随后可执行某些操作，如拒收或标记邮件等。
- DNS 黑名单。允许指定多个 DNS 黑名单服务，每当有人试图向服务器发送邮件时将核对该黑名单。如果连接 IP 已被主机列入黑名单，则将拒收该邮件。

（5）【安全设置】命令可配置的安全功能很多，主要包括：

- 中转控制。用来控制当到达邮件服务器的邮件并非由本地地址所收发时，MDaemon 将采取的操作。
- IP 防护。如果在此列表中指定的域名试图连接到服务器，其 IP 地址必须与已指派给它的相匹配。
- SMTP 身份验证。用来设置多个选项，以指示当向 MDaemon 发送邮件的用户已经或尚未通过身份验证时，MDaemon 将如何操作。
- 反向查询。MDaemon 可查询 DNS 服务器以检验在入站邮件中上报的域名和地址的有效性。该界面上的控件可用于拒绝可疑邮件或向其插入特殊报头。在 MDaemon 日志中也会报告反向查询数据。
- POP 先于 SMTP。该界面上的控件用来要求每个用户在被允许发送邮件到 MDaemon 之前必须首先访问其邮箱，这样就验证了用户是有效账户持有人并可使用该邮件系统。
- 可靠主机。被视为中转控制界面上所列中转规则的例外情况的域名和 IP 地址。



- SPF/Sender ID。所有域都发布 MX 记录来标识可接收邮件的计算机，但这并未标识允许发送邮件的位置。使用 Sender Policy Framework(SPF)和 Sender ID，域还可发布“反向 MX”记录以标识被授权发送邮件的位置。
- DomainKeys 和 DomainKeys Identified Mail。DomainKeys(DK)和 DomainKeys Identified Mail(DKIM)是一种可用来防止欺诈的邮件验证系统，还可用来确保入站邮件的完整性，以保证邮件从离开发件人的邮件服务器直到抵达用户服务器的过程中未被篡改。这可通过使用加密的公钥/私钥配对系统来实现。出站邮件用私钥进行签名，而入站邮件通过使用发件人 DNS 服务器上发布的公钥测试其签名来进行验证。
- 认证。邮件认证指的是一个实体“担保”或“证明”另一个实体的良好邮件传输品行。认证功能非常有用，因为有助于确保邮件将不会错误地或不必要地经受不当的垃圾邮件过滤器的分析，还有助于降低处理每封邮件所需的资源。
- 地址黑名单。不允许所列地址发送邮件到服务器。
- IP 屏蔽。用来指定允许或拒绝连接到服务器的 IP 地址。
- 主机屏蔽。用来指定允许或拒绝连接到服务器的主机(域名)。
- 动态屏蔽。使用动态屏蔽功能，MDaemon 可以追踪发送服务器的行为，以便识别可疑的行为并做出相应的响应。例如，在来自某个 IP 地址的邮件连接过程时，一旦出现了指定数量的“未知收件人”错误，则可暂时禁止该 IP 地址，使其今后无法连接到服务器。
- SSL 和 TLS。MDaemon 支持用于 SMTP、POP、IMAP 以及 WorldClient 网络服务器的安全套接字层(SSL)协议。SSL 是保护服务器/客户端 Internet 通信安全的标准方案。
- 反向散射保护。反向散射指的是用户收到对其从未发送过的邮件的响应邮件。当垃圾邮件或病毒发送的邮件中包含伪造的“返回路径”地址时就会发生反向散射。反向散射保护使用私钥散列方法生成，并将特殊的时间敏感代码插入到用户外发邮件的“返回路径”地址中，以确保只向账户投递合法的投递状态通知和自动应答，从而有助于防止发生这种情况。
- 带宽节流。带宽节流功能能控制 MDaemon 占用消耗的带宽。可以控制会话或服务的进展速率，按域(包括默认域、额外域和域网关)为 MDaemon 提供的每个主要服务设置不同的速率。
- 缓送。一旦从邮件发件人处收到指定数量的 RCPT 命令，就可有意延迟连接。这是为了阻止垃圾邮件制造者试图发送未经请求的群发电子邮件。该技术背后的设想是如果垃圾邮件制造者发送每封邮件都需要花费相当长的时间，这将迫使他们以后不再重复同样的操作。
- 灰名单。灰名单是一种抵御垃圾邮件的技术，它利用了 SMTP 服务器会重试投递任何收到暂时(即“稍后重试”)错误代码的邮件这一特性。通过这项技术，当邮件来自未列入白名单或先前未知的发件人时，其发件人、收件人和发送服务器的 IP 地址会被记入日志，然后在 SMTP 会话期间将由灰名单以暂时错误代码拒绝该邮件。几分钟以后，当合法服务器试图再次投递该邮件时，它们将被接受。因为垃圾邮件



制造者通常不会进一步尝试投递，灰名单有助于显著减少用户收到的垃圾邮件数量。

- HashCash。HashCash 是一种“工作证明”系统，它类似于电子邮票，既是一个反垃圾邮件工具，也是一个拒绝服务对策。使用 HashCash 系统，MDaemon 能制造 HashCash 邮票，它事实上是由 CPU 处理时间而不是实际货币来“缴付”的。HashCash 邮票被插入到出站邮件报头中，然后由收件人的邮件服务器进行验证并根据票面价值来权衡。加盖邮戳的邮件是合法邮件的可能性更大，因而能通过收件人服务器的反垃圾邮件系统。
- LAN IP 地址。使用该界面列出 LAN(局域网)上的 IP 地址。为了带宽节流的目的，这些 IP 地址被视作本地通信地址，并可免除其他各种安全和垃圾邮件防范限制。
- 站点策略。用来创建站点策略，并在每个 SMTP 邮件会话开始时，将其传输到发送服务器。常用站点策略的一个范例是“该服务器不支持中转”。

与基本配置类似，安全配置实际上真正需要设置的选项并不是很多，大部分都采用默认值即可。下面仅以反病毒的设置进行说明：

(1) 在 MDaemon 程序主界面中打开【安全】菜单，如图 6-35 所示。

(2) 选择 AntiVirus 命令，弹出【内容过滤器】对话框。此时左侧窗格默认选中【反病毒】选项，可以在右侧进行相关设定，如图 6-36 所示。

提示：由图 6-36 可以看出，MDaemon 的内嵌防病毒插件 SecurityPlus 实际使用的是著名的卡巴斯基的反病毒引擎。



图 6-36 【反病毒】选项

(3) 在左侧窗格选择【反病毒更新程序】选项，如图 6-37 所示。此时再单击下方的【调度程序】按钮。

(4) 弹出【事件调度】对话框，如图 6-38 所示。此时就可以设定自动更新时间表，通常默认已有升级时间安排为每天 11 点左右。单击【确定】按钮，完成设置。





图 6-37　【反病毒更新程序】选项



图 6-38　【事件调度】对话框

6.3.3　邮箱账户管理

邮件服务器安装设置完毕后，接下来需要对邮箱账户进行管理，包括账户的创建、修改以及删除等操作。对账户的管理是通过主界面中的【账户】菜单进行的。

（1）在 MDaemon 程序主界面中打开【账户】菜单，如图 6-39 所示。

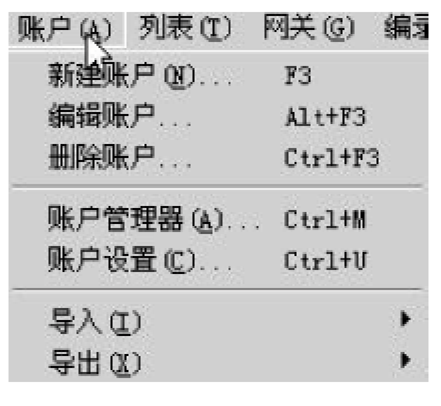


图 6-39　【账户】菜单

（2）新建账户。选择【新建账户】命令，会弹出【账户】对话框，如图 6-40 所示。在这里首先创建一个名为 test 的邮箱账户。在【姓名】文本框中输入用户名全称（此处为 test），在【E-mail 地址】文本框中输入用户 ID（此处为 test.），如果 MDaemon 设置了多个域名，那



么在添加用户的时候还要选择将用户名添加到某一个域名之下。在【E-mail 密码】文本框中输入用户密码(此处仍为 test)。其余选项采用默认设置,单击【确定】按钮。



图 6-40 【账户】对话框—新建账户

此时因为刚才输入的密码 test 不是强密码,那么在默认配置下,会弹出【信息】对话框提示重新输入密码,如图 6-41 所示。强密码其实只要满足大小写+数字就可以通过,如 Password。这里为了输入简单,在【账户设置】对话框中关闭强密码要求,使其不再提示(具体方法后述)。



图 6-41 【信息】对话框

这样就完成了 test 账户的创建。

用同样步骤,再新建 a、b 两个账户,密码分别为 a、b。

(3) 编辑账户。账户创建后,可以随时对账户参数进行相关设置。选择【编辑账户】命令,同样会弹出【账户】对话框,如图 6-40 所示。在左侧窗格选择相应选项,就可以在右侧窗格进行相关设置。这里以常用的【配额】和【Web 访问】两个选项为例进行说明。

在左侧窗格选择【配额】选项,如图 6-42 所示。

下面对其中的选项一一说明。

- 该账户必须遵守这些配额设置。启用磁盘配额控制,以表示该用户账户必须遵循磁盘配额设定。
- 每次存储邮件的最大数目。允许信箱中同时存放的邮件总数。
- 允许的最大磁盘空间。设置了用户所能使用的最大信箱容量。
- 使用域默认设置。MDaemon 支持自动删除账户以及邮件的功能。默认情况下,此项功能是被关闭了的。如果需要,可以将此功能打开,即取消对【使用域默认设置】复选框的选择。取消该复选框之后,下面的三个设置项目将变为可设置形式。
- 自动删除账户当处于非活动状态达×天(0=从不)。用来设置自动删除非使用账户的选项。如果在这里填写上 30,就表示当用户在 30 天内都不对信箱进行访问,系统



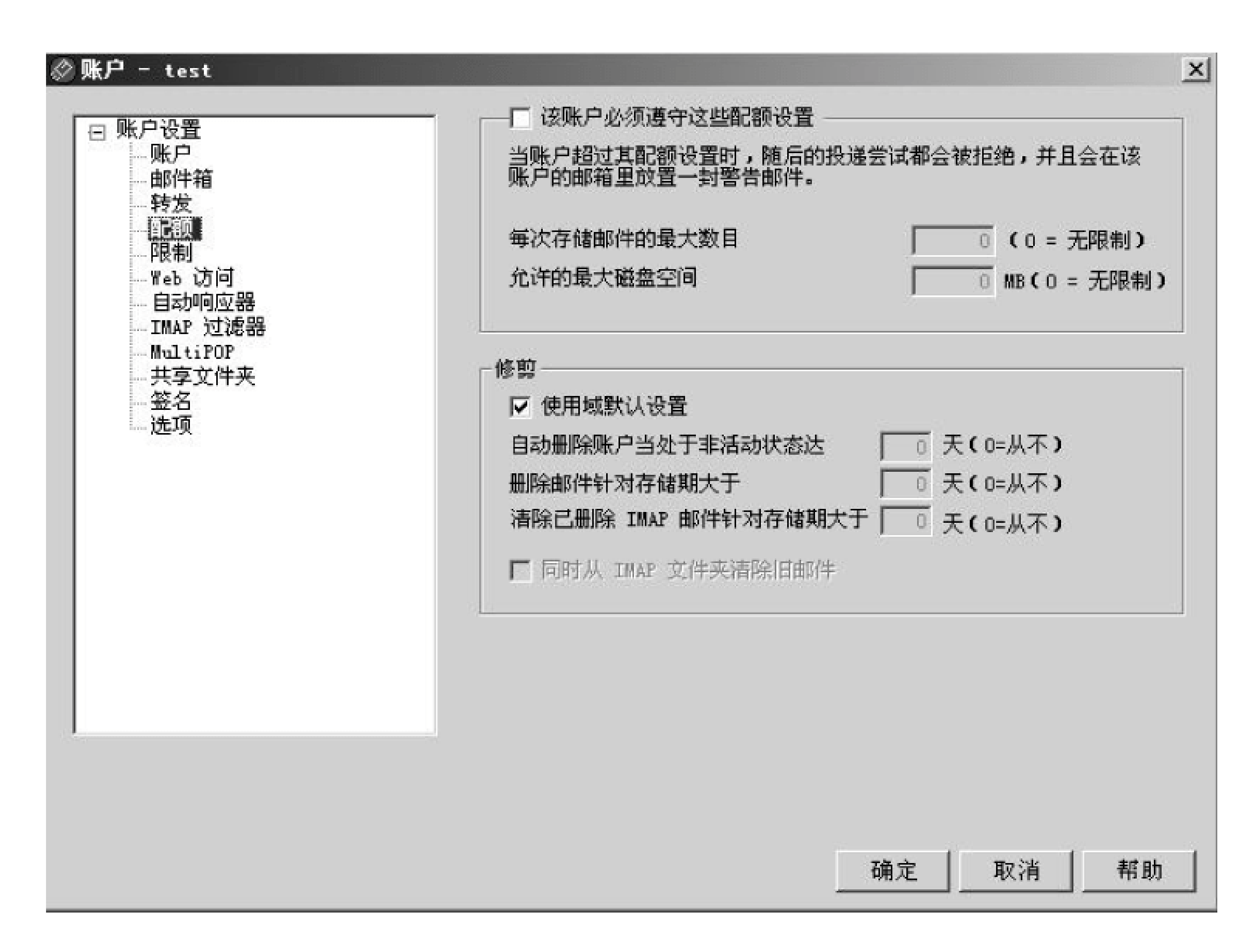


图 6-42　【账户】对话框—【配额】选项

将自动删除该账户。如果设置为 0,则表示永远不删除该账户。

- 删除邮件针对存储期大于×天(0=从不)。用来设置自动删除旧邮件。如果设置为 30,就表示系统将自动删除已经存放在信箱里超过 30 天的邮件。若设置为 0,则表示不删除。
- 清除已删除 IMAP 邮件针对存储期大于×天(0=从不)。用法和上一项类似,只不过这里是针对 IMAP 邮件而言的。

在左侧窗格选择【Web 访问】选项,如图 6-43 所示。下面对其中的选项一一说明。

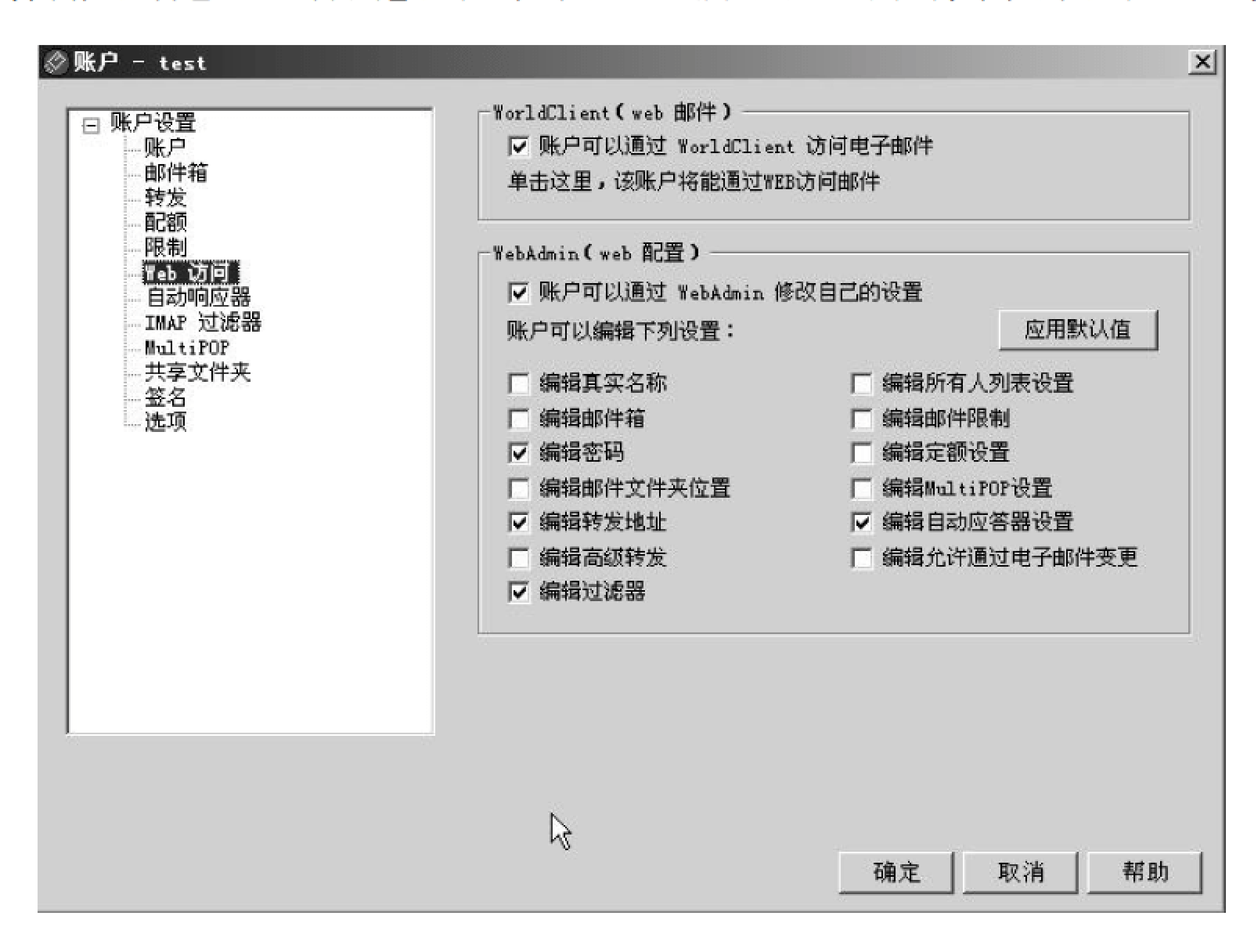


图 6-43　【账户】对话框—【Web 访问】选项



- 【WorldClient(web 邮件)】选项区域。默认情况下,MDaemon 程序允许所有的用户都能以 Web Mail 方式来访问自己的信箱。如果有不同的需要,则可以取消选中【账户可以通过 WorldClient 访问电子邮件】复选框。
- 【WebAdmin(web 设置)】选项区域。如果允许用户登录上 WebMail 之后可对自己的资料和设置进行修改,那么在这里就一定要选中【账户可以通过 WebAdmin 修改自己的设置】复选框。
- 编辑真实名称。是否允许用户修改自己的真实姓名。
- 编辑邮件箱。是否允许用户修改其邮件地址的邮件箱部分。
- 编辑密码。是否允许用户修改自己的个人信箱密码(建议允许)。
- 编辑邮件文件夹位置。是否允许用户修改个人邮件存放位置。
- 编辑转发地址。是否允许用户修改转寄邮件地址(建议允许)。
- 编辑高级转发。是否允许用户修改转寄高级选项内容。
- 编辑过滤器。是否允许用户创建并管理自己的邮件过滤器(建议允许)。
- 编辑所有人列表设置。是否允许用户修改全体人员邮寄列表设定。
- 编辑邮件限制。是否允许用户修改邮件限制设定。
- 编辑定额设置。是否允许用户修改个人磁盘配额设定。
- 编辑 MultiPOP 设置。是否允许用户修改多重 POP 设定。
- 编辑自动应答器设置。是否允许用户修改自动回复设定(建议允许)。
- 编辑允许通过电子邮件变更。是否允许用户通过邮件进行设定。

在用户参数设置完毕后,单击【确定】按钮,保存参数设置并退出。

(4) 账户管理器。账户管理器能够更好地管理所有的账户操作,包括选择、添加、删除或者修改账户等。它还能根据邮件箱、域、真实名称或者邮件文件对账户进行分类。选择【账户管理器】命令,会弹出【账户管理器】对话框,如图 6-44 所示。



图 6-44 【账户管理器】对话框

可以看出,在对话框上部可以选择显示的账户范围和搜索选项,中间显示的是账户列表,窗口下部显示的是可以进行的账户操作。列表中的每一个条目都包含了一个账户状态图标、邮件箱、所属域、账户持有人的真实名称、账户所属的任何群组以及存储账户邮件的邮





件文件夹等信息，且都可以以升序和降序的方式排列，默认一次最多能在此列表中显示 500 个账户。这里显示了刚才新建的 a、b、test 三个完全访问账户，以及安装时创建的 admin 全局管理员账户和系统自动生成的 MDaemon 系统账户。

在列表中选定账户后，单击右下方的功能按钮，就会调用其【账户】对话框进行相应操作。其具体界面与前述相同，在此不再赘述。

（5）账户设置。选择【账户设置】命令，弹出【账户设置】对话框，如图 6-45 所示。在这里可以设置账户的一些共性特征，包括新建账户默认值、自动应答器等。此处设置的参数将应用于以后创建的所有账户。实际上，前面所述对账户的操作都是调用了相应账户的【账户设置】对话框。



图 6-45　【账户设置】对话框

如前所述，在这里还可以设置关闭强密码要求。

关闭强密码要求的设置步骤如下：

在图 6-45 所示左侧窗格中选择【新建账户默认值】→【邮件箱】选项，在右侧窗格中取消选中【需要强密码】复选框，单击【确定】按钮即可。

6.3.4　客户端测试

前面创建的 MDaemon 邮件服务器的主域是 test.com，三个完全访问邮箱账户分别是 a@test.com、b@test.com 和 test@test.com，那么在邮件服务器安装设置完毕，并且创建了相应的邮箱账户后，就可以在电子邮件客户端进行收发邮件的测试了。

1. 在客户端建立电子邮件账户

Outlook Express 是 Windows Server 2003 内置的邮件客户端，也是一款常用的邮件客户端。下面就以 Outlook Express 为例进行说明。



（1）在 Outlook Express 中打开【工具】菜单，如图 6-46 所示。



图 6-46 Outlook Express 的【工具】菜单

（2）选择【账户】命令，此时会弹出【Internet 账户】对话框，如图 6-47 所示。在该对话框中单击【添加】按钮，选择其级联菜单中的【邮件】命令。

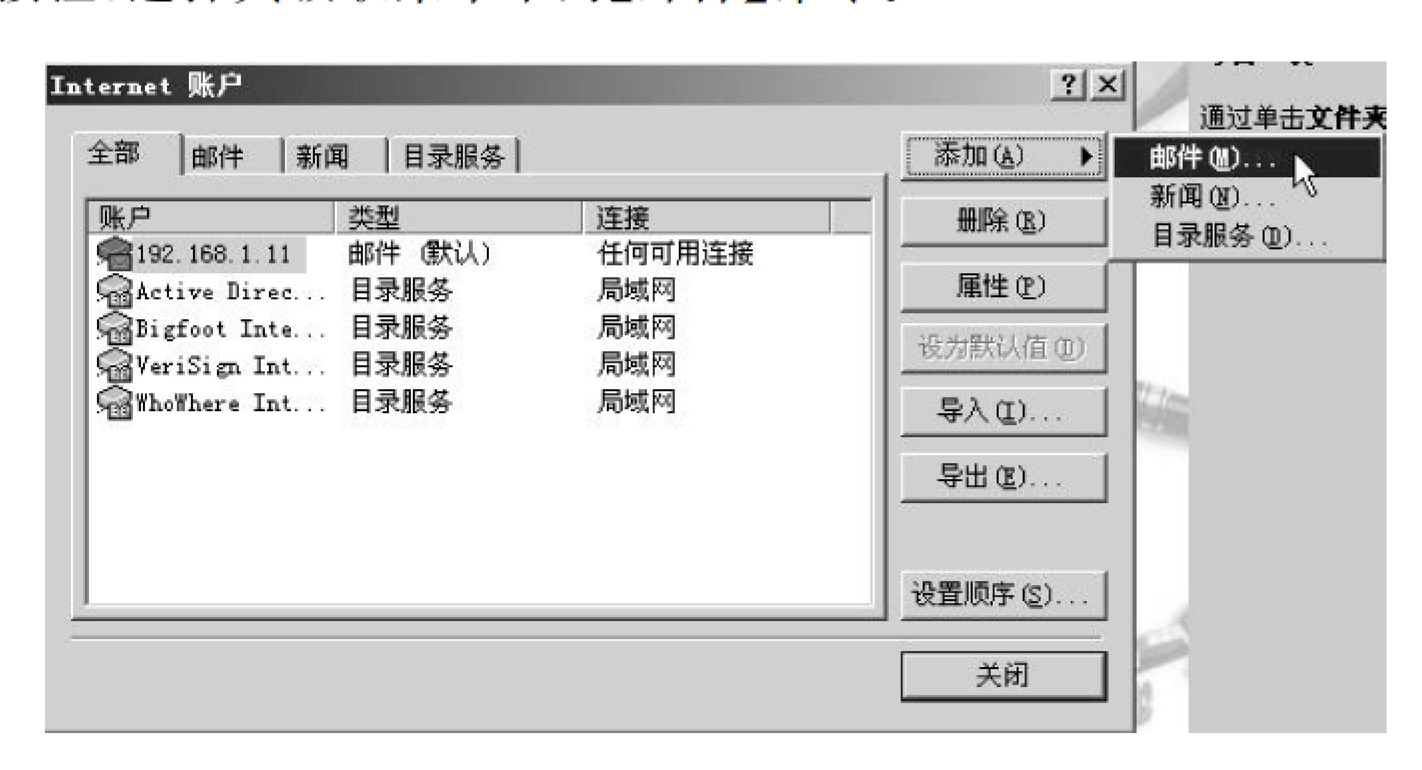


图 6-47 【Internet 账户】对话框

（3）此时弹出【Internet 连接向导】对话框，如图 6-48 所示。这里首先添加 test 账户。在【显示名】文本框中输入 test，单击【下一步】按钮。

（4）此时的【Internet 连接向导】对话框如图 6-49 所示。在【电子邮件地址】文本框中输入 test@test.com，单击【下一步】按钮。

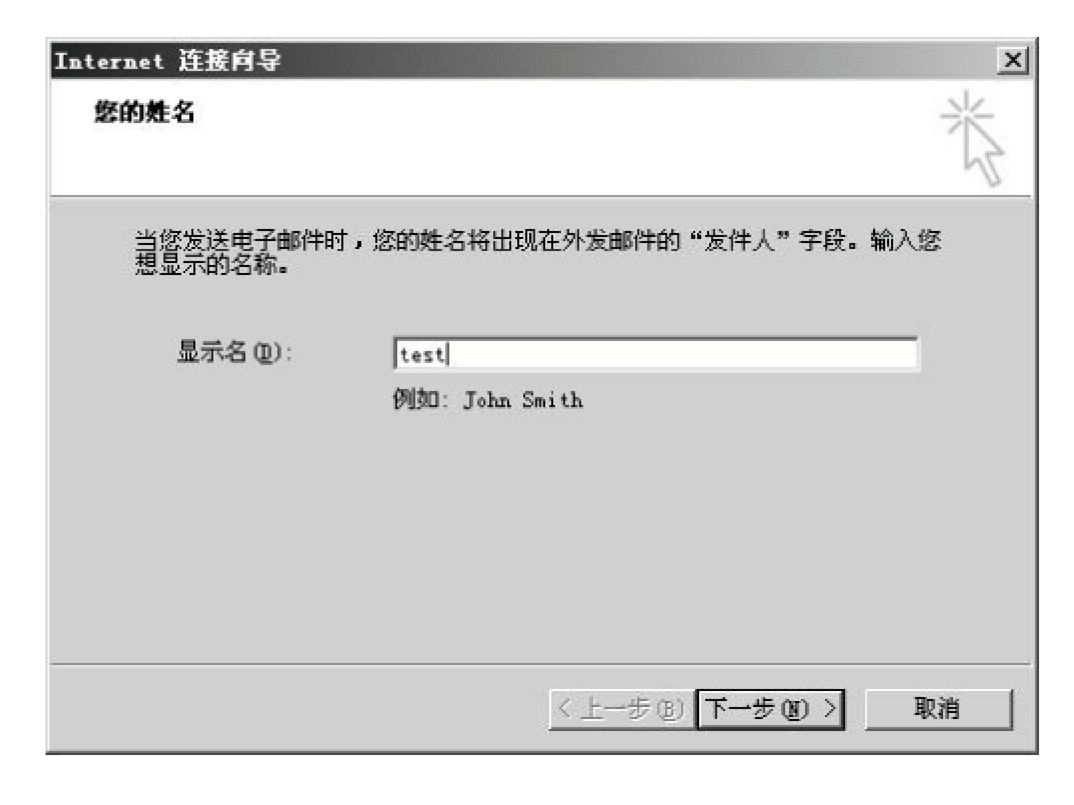


图 6-48 【Internet 连接向导】对话框——填写显示名



图 6-49 【Internet 连接向导】对话框——填写电子邮件地址



(5) 此时的【Internet连接向导】对话框如图6-50所示。【我的邮件接收服务器是】选择POP3服务器，然后在【接收邮件(POP3,IMAP或HTTP)服务器】和【发送邮件服务器(SMTP)】两个文本框中均输入MDaemon服务器的IP地址192.168.1.11，单击【下一步】按钮。

(6) 此时的【Internet连接向导】对话框如图6-51所示。在【账户名】和【密码】两个文本框中均输入test，并选中【记住密码】复选框，单击【下一步】按钮。

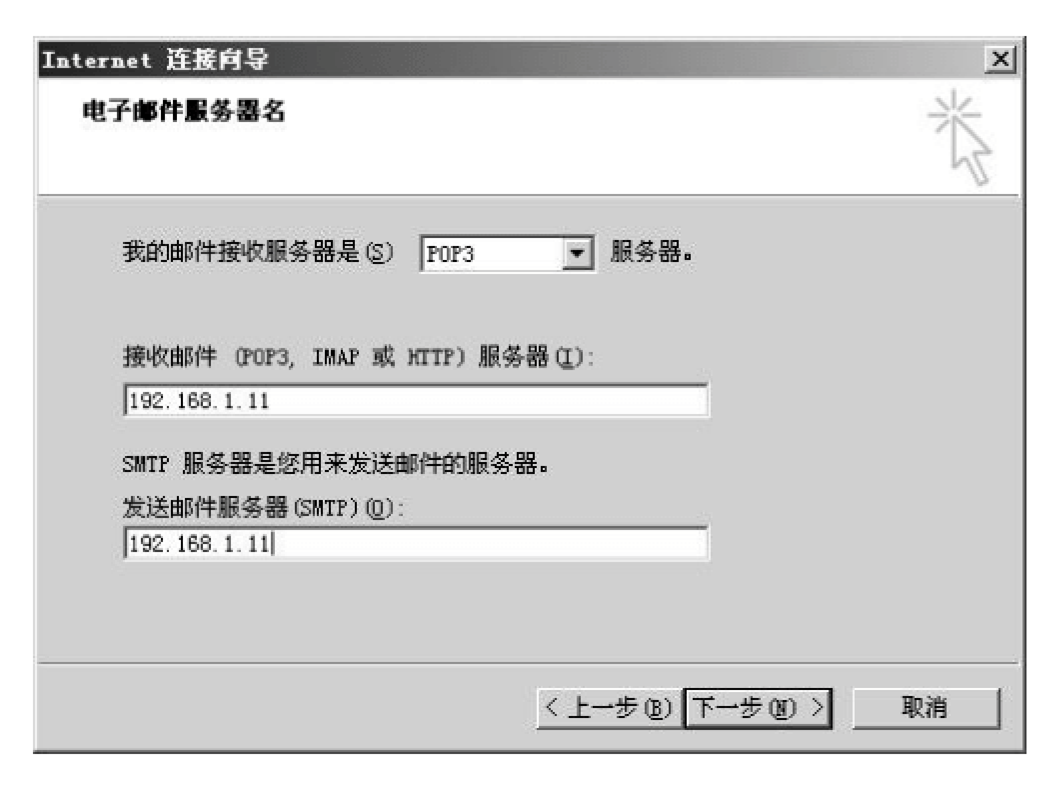


图6-50　【Internet连接向导】对话框——填写电子邮件服务器名

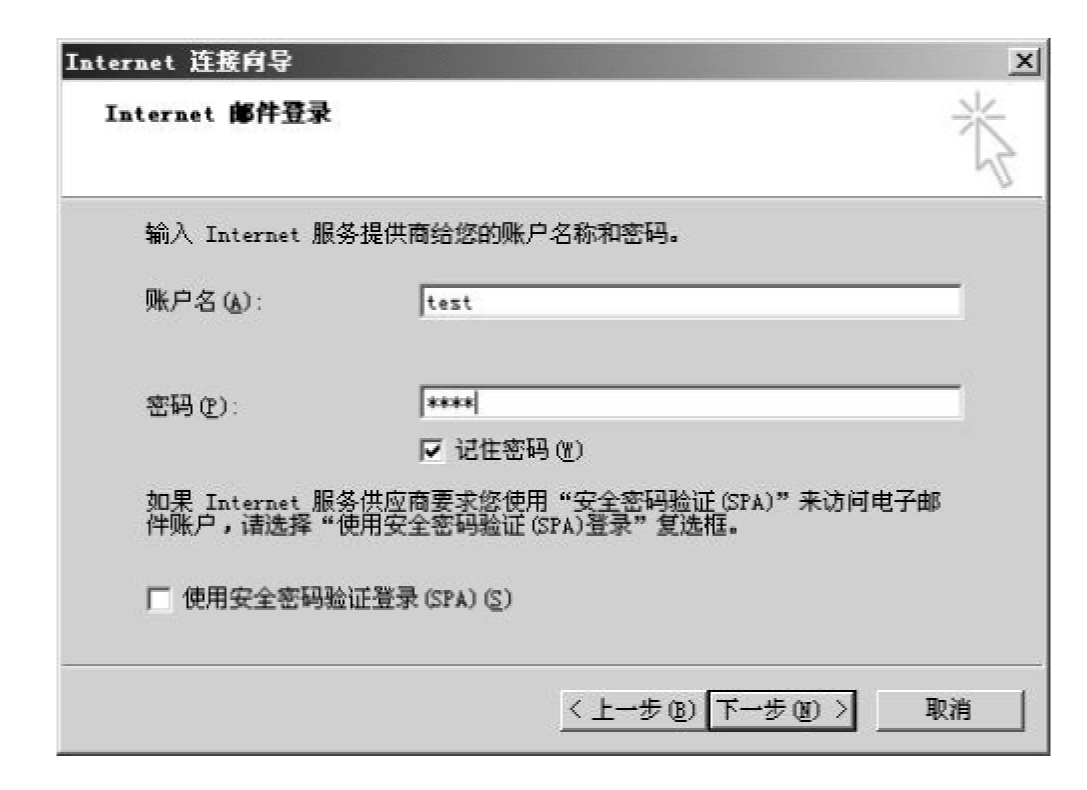


图6-51　【Internet连接向导】对话框——填写邮件登录信息

(7) 此时的【Internet连接向导】对话框如图6-52所示。至此，邮件账户test已经建立，单击【完成】按钮。

(8) 此时在【Internet账户】对话框中会出现刚才新建立的邮件账户，如图6-53所示。选择该账户，单击【属性】按钮。



图6-52　【Internet连接向导】对话框——完成账户信息录入

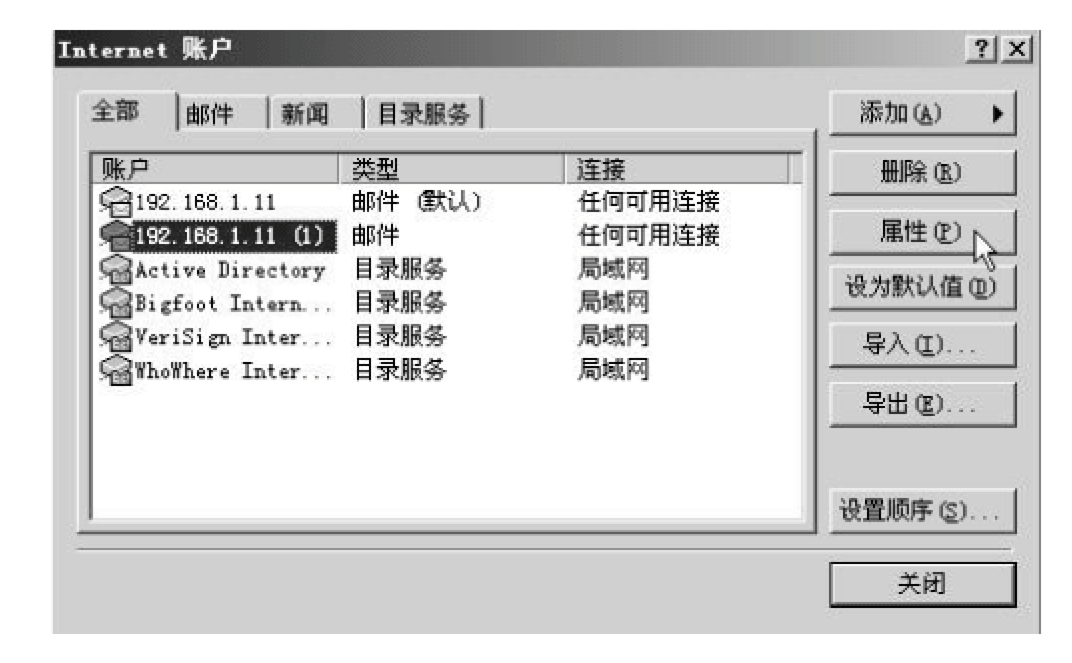


图6-53　【Internet账户】对话框

(9) 此时弹出【账户属性】对话框，如图6-54所示。这里首先将【邮件账户】文本框的内容更改为MDaemon Mail Server，然后在【答复地址】文本框中输入test@test.com。填写完毕后，选择【服务器】选项卡。

(10) 此时【账户属性】对话框如图6-55所示。在这里选中【我的服务器要求身份验证】复选框，然后单击右侧的【设置】按钮。



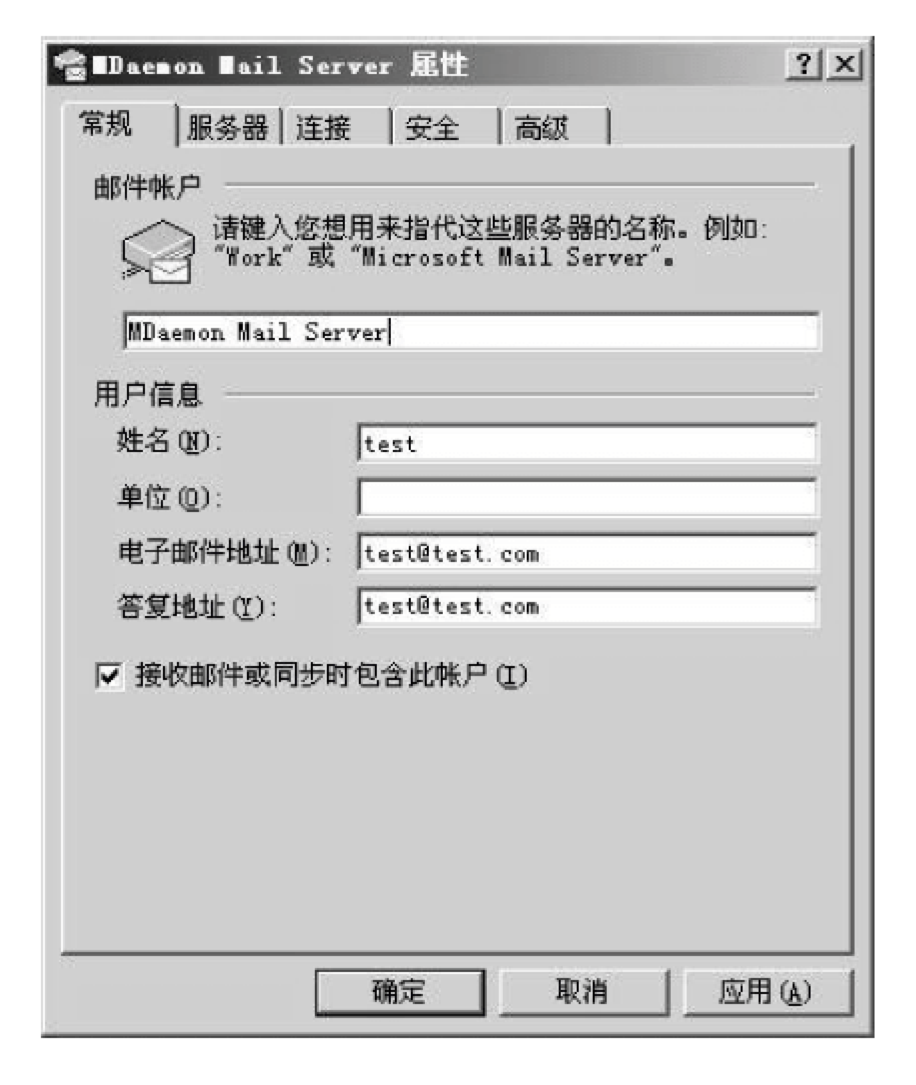


图 6-54 【账户属性】对话框——【常规】选项卡

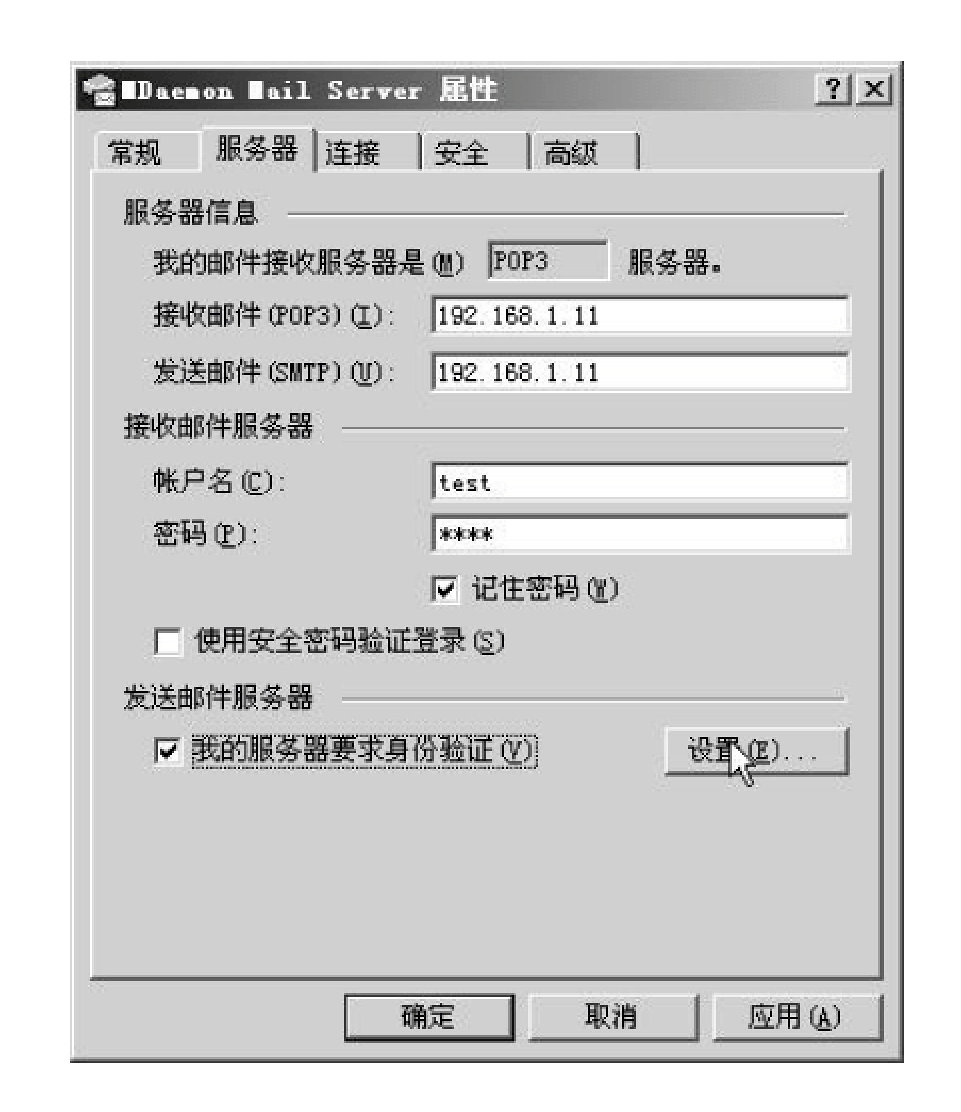


图 6-55 【账户属性】对话框——【服务器】选项卡

(11) 此时弹出【发送邮件服务器】对话框，如图 6-56 所示。在【登录信息】选项区域中选中【使用与接收邮件服务器相同的设置】单选按钮，再单击【确定】按钮。至此就完成了 test 账户在 Outlook Express 中的设置。

(12) 以相同方法再在 Outlook Express 中分别设置 a、b 两个邮箱账户，此时查看【Internet 账户】对话框的【邮件】选项卡，如图 6-57 所示。

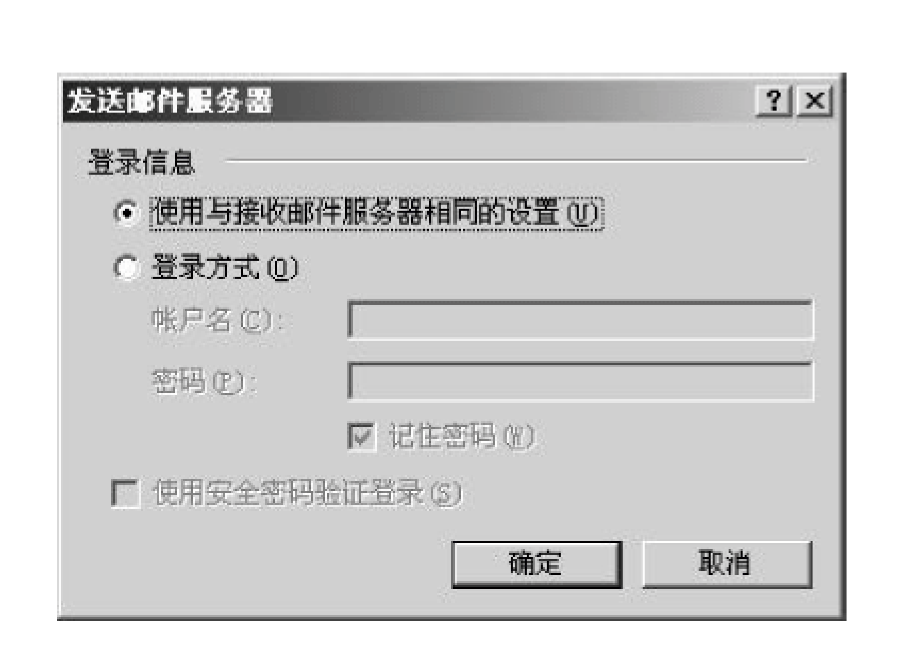


图 6-56 【发送邮件服务器】对话框



图 6-57 【Internet 账户】对话框——【邮件】选项卡

2. 在客户端进行测试

(1) 使用 test 用户给 a 用户写一封信，同时抄送给 b 用户，信的主题为 Test，内容为 "This is only a test!"，如图 6-58 所示。

(2) 单击【发送】按钮，信件成功发送。此时查看【已发送邮件】文件夹，如图 6-59 所示，表明发送邮件成功。

(3) 此时在 Outlook Express 中打开【工具】菜单，选择【发送和接收】命令，在级联菜单中选择 a，接收 a 用户的邮件，如图 6-60 所示。







图 6-58　撰写邮件



图 6-59　查看【已发送邮件】文件夹



图 6-60　接收 a 用户的邮件

(4) 此时查看【收件箱】文件夹，可以看到，a 用户收到来自 test 用户的一封新邮件，信的主题为 Test，内容为“This is only a test!”，如图 6-61 所示。这表明客户端测试成功。



图 6-61　查看【收件箱】文件夹



6.4　Web 远程管理 MDaemon 服务器

MDaemon 提供了 Web 远程管理功能插件 WebAdmin。WebAdmin 是一个服务器应用程序，设计成与 MDaemon 在同一台计算机上的后台运行。要访问 WebAdmin，只要打开浏览器并将其指向 WebAdmin 所在的 URL 与端口号(如 http://mail_server_ip_address:1000)即可。通过 WebAdmin，管理员账户可以像在本地一样来管理和操作 MDaemon 服务器。WebAdmin 提供了多语言支持，并且可以通过修改语言配置文件来个性化人机交互界面，还可以为每个邮件域分配一个管理员，使其能够自行管理自己的邮件域，极大地方便了管理，并且非常灵活。依据登录用户访问级别的不同，其能够远程管理和设置 MDaemon 的权限也不相同。WebAdmin 用户具有三种访问级别：全局、域和用户。

- 全局管理员。全局管理员是那些拥有全局访问许可的用户，可以在 MDaemon 中的账号设置下启用。全局访问意味着用户可以通过 WebAdmin 查看和配置任何可以访问的设置与控制。全局管理员可以添加、编辑和删除用户、域和邮件列表。可以编辑产品的 INI 文件，指定其他用户作为域管理员，管理密码，拥有完全的管理控制权限。
- 域管理员。与全局管理员类似，域管理员通过 WebAdmin 拥有对所有用户和可访问的产品设置的完全管理权。然而其管理控制权是受到域或者被给定访问的域的限制。域管理员及其所控制的域是从 WebAdmin 中由全局管理员指定的，或者由另外一个可以访问那些域的管理员指定的。
- 用户。用户访问是 WebAdmin 访问中的最低级别。例如，MDaemon 用户可以登录到 WebAdmin，并查看其个人账户设置以及编辑其个人 MultiPOP 条目、邮件过滤器、自动回复等。可进行编辑的设置类型和数量取决于每位用户的账户设置中被赋予的权限。

下面以远程创建邮箱账户 c 的操作为例进行具体说明。

(1) 在 Web 浏览器地址栏中输入 http://mail_server_ip_address:1000(这里为 http://192.168.1.11:1000)并按 Enter 键，将显示 WebAdmin 登录窗口。此时在 E-mail Address 文本框中输入在 MDaemon 安装时创建的全局管理员账户 admin，在【密码】文本框中输入相应密码 123456，在【语言】下拉列表框中选择 Chinese，如图 6-62 所示。单击【登录】按钮。

(2) 此时进入远程管理界面，系统首先显示服务器状态信息，如图 6-63 所示。从图中可以看到，WebAdmin 的界面与 WorldClient 的界面基本相同，都是在左侧选择相应功能选项，在右侧进行相关操作。左侧选项包括【主菜单】、【设置】、【安全】、Log/Config Files、【注销】等诸多功能，在本地服务器上进行的所有操作设置都能够通过远程管理实现。

(3) 要创建新账户，首先在左侧单击【主菜单】选项中的【用户】超级链接，此时界面如图 6-64 所示。它实际上相当于服务器上的【账户管理器】界面，列出了系统当前存在的所有账户。在此界面可以实现对账户的新建、编辑、删除以及导入/导出等操作。这里单击【新建】超级链接进行账户的创建。





图 6-62　WebAdmin 登录窗口



图 6-63　WebAdmin 界面——状态

(4) 此时弹出【Alt-N WebAdmin—网页对话框】窗口，如图 6-65 所示。在【姓名】文本框中输入 c，在【E-mail 地址】文本框中输入 c@test.com，在【邮件密码】文本框中输入 c，其余选项采用默认值，单击【保存】超级链接。



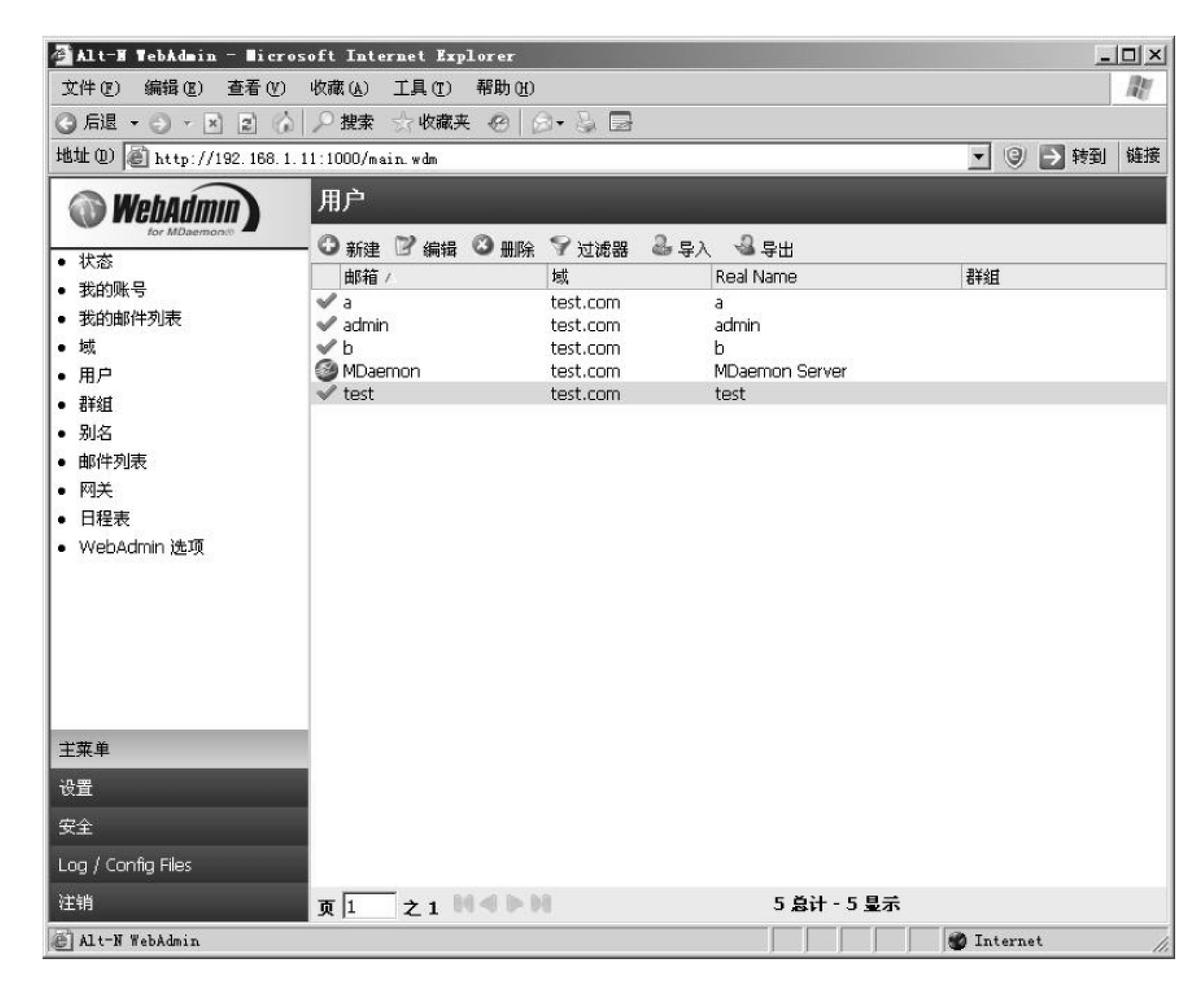


图 6-64 WebAdmin 界面——用户

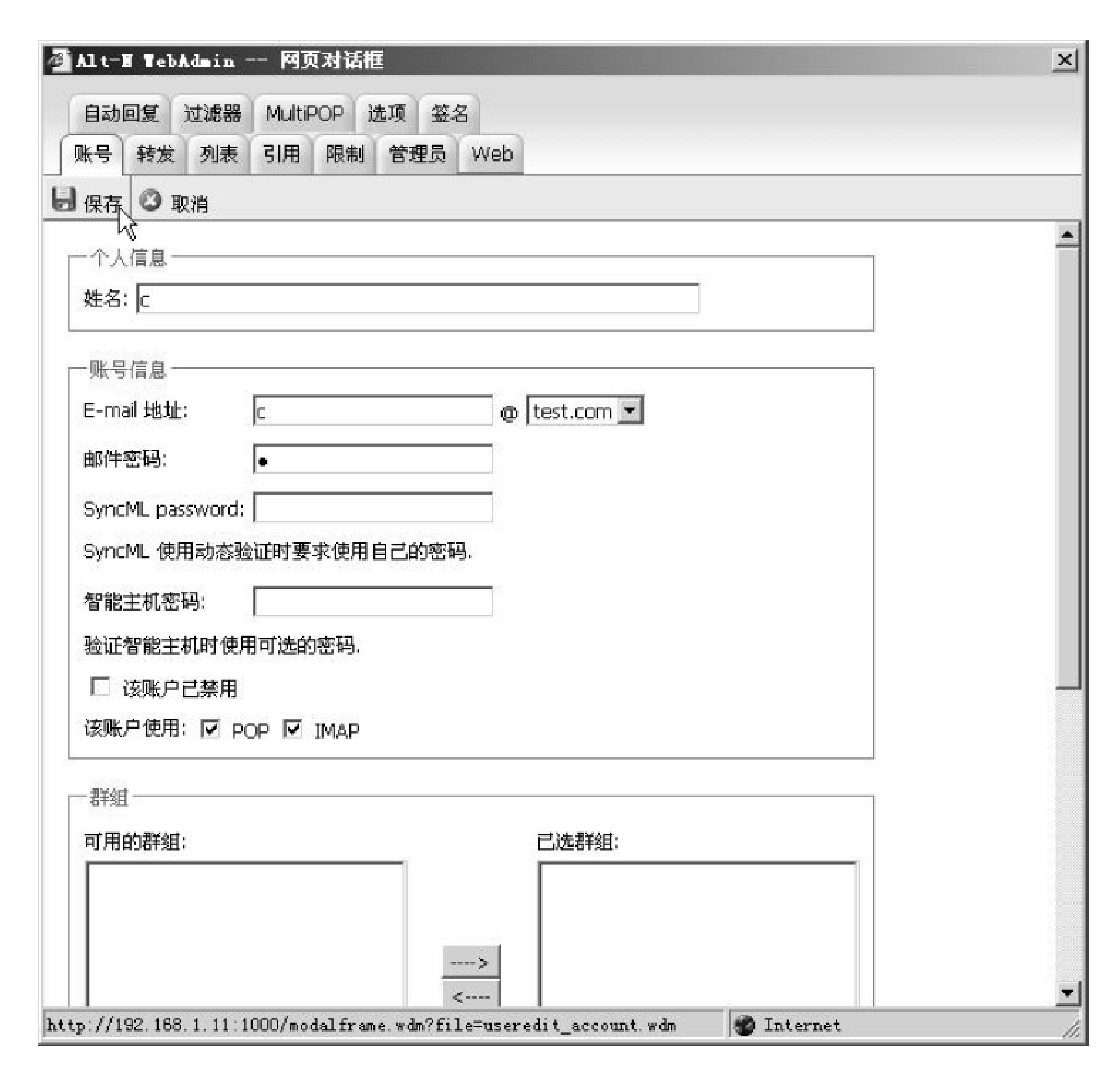


图 6-65 【Alt-N WebAdmin—网页对话框】窗口



(5) 此时弹出信息提示对话框，提示账户创建成功，如图 6-66 所示。单击【确定】按钮返回。



图 6-66　信息提示对话框

(6) 此时在服务器端 MDaemon 程序主界面中打开【账户】菜单，然后选择【账户管理器】命令，会弹出【账户管理器】对话框，如图 6-67 所示。从中可以看出，已经在服务器上成功创建了邮箱账户 c。



图 6-67　【账户管理器】对话框

6.5　通过 WorldClient 实现 Web 邮件服务

MDaemon 邮件服务器收发电子邮件可以分别采用 Web 方式及 POP 方式来实现。WorldClient 就是 MDaemon 的 WebMail 服务。WorldClient 默认使用的是仿微软 Office Outlook 的操作界面，它几乎包含了微软 Office Outlook 的所有功能，如日历、联系人、任务及便签等，而且 MDaemon 提供的 Outlook Connector 插件能够无缝地与微软 Office Outlook 结合使用。最重要的是 MDaemon 从 v9. x 开始就增强了与微软活动目录的集成，不仅可以满足中小企业 Internet 的邮件需求，还可以满足 Intranet 的内部邮件需求。

6.5.1　以自服务方式运行 WorldClient

所谓自服务方式，指的是 WorldClient 使用自己默认的端口号(3000)提供服务，这样要访问默认的 WorldClient 网页就需要使用形如 http://mail_server_ip_address:3000 这样的方式。这也是默认的使用方式。

下面以收发邮件的操作为例进行具体说明：

(1) 在 Web 浏览器地址栏中输入 http://mail_server_ip_address:3000(这里为 http://192.168.1.11:3000)并按 Enter，将显示 WorldClient 登录窗口。此时在【邮件地址】文本框中输入之前创建的完全访问账户 test，在【密码】文本框中输入相应密码 test，在【语言】下拉列表框中选择 Chinese 选项，在【方案】下拉列表框中选择 Standard 选项，如图 6-68 所示。单击【登录】按钮。





图 6-68 WorldClient 登录窗口

(2) 此时系统进入 test 的用户信箱界面,如图 6-69 所示。从中可以看到,WorldClient 的界面与 163、Gmail、Hotmail 等电子邮件的界面基本相同,都是在左侧选择相应功能选项,在右侧进行相关操作。



图 6-69 WorldClient 的用户界面

在左侧选择【撰写】选项,撰写一封新邮件。

(3) 此时系统进入撰写新邮件界面,如图 6-70 所示。这里使用 test 用户给 a 用户写一封信,信的主题为 Test2,内容为“Hello!”。



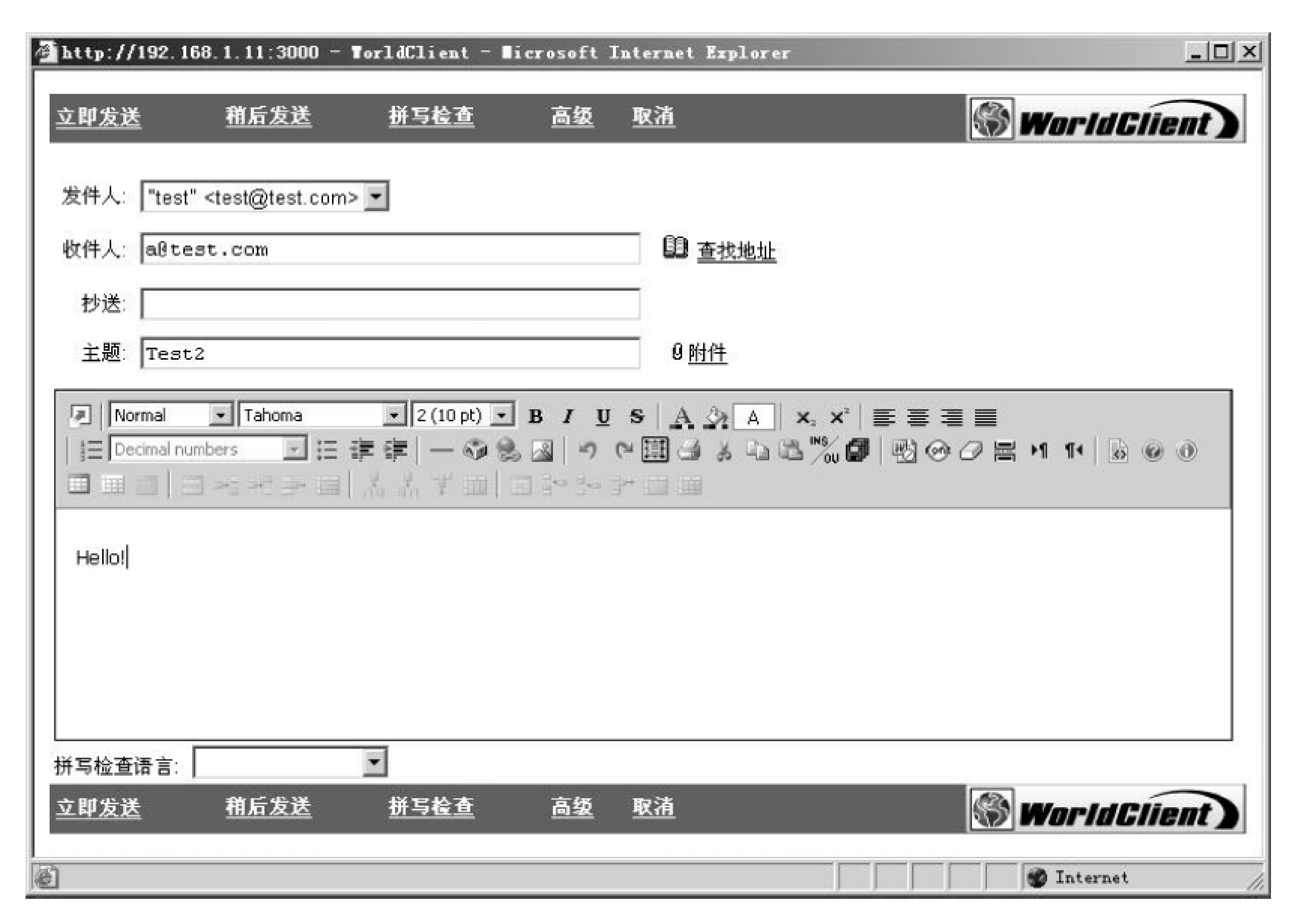


图 6-70　撰写新邮件界面

(4) 单击【立即发送】超级链接,信件成功发送。此时在左侧选择【已发送邮件】选项,在右侧查看【已发送邮件】文件夹内容,如图 6-71 所示,确实有一封主题为 Test2 的邮件,表明发送邮件成功。



图 6-71　查看已发送邮件

(5) test 用户单击左侧【退出】选项,退出登录。接着 a 用户重新登录,进入 a 用户的信箱界面,如图 6-72 所示。可以看到,此时 a 的【收件箱】里有一封来自 test 用户、主题为 Test2 的新邮件。





图 6-72　查看收件箱

（6）单击该邮件进行查看，进入查看邮件界面，如图 6-73 所示。从中可以看到，信的主题为 Test2，内容为“Hello！”，表明系统收发邮件正常。



图 6-73　查看邮件

为了更方便用户的收发操作，还可以改变其中的相关参数。单击左侧的【选项】选项，右侧会显示信箱的相应参数，可以进行相应的修改。在修改完成之后，单击【完成】超级链接，





以保存所做的修改即可。因相关操作过程与163、Gmail、Hotmail等电子邮件的操作基本相同，在此不再赘述。

6.5.2　以其他ISAPI方式运行WorldClient

当用户需要将WorldClient的端口改为80端口，而此服务器上还架设了其他的网站，使用的也是80端口，此时就需要以其他ISAPI方式运行WorldClient。以常见的IIS为例，将WorldClient运行于IIS下，就可以像访问一般网站一样，使用形如http://mail_server_ip_address这样的方式，来访问WorldClient的网页。

具体设置步骤如下：

(1) 打开IIS，新建一个应用程序池。在Windows 2003系统中依次选择【开始】→【控制面板】→【管理工具】→【Internet信息服务(IIS)管理器】，会弹出【Internet信息服务(IIS)管理器】窗口。从左侧树状列表中选择【应用程序池】，右击，在弹出的快捷菜单中依次选择【新建】→【应用程序池】命令，如图6-74所示。

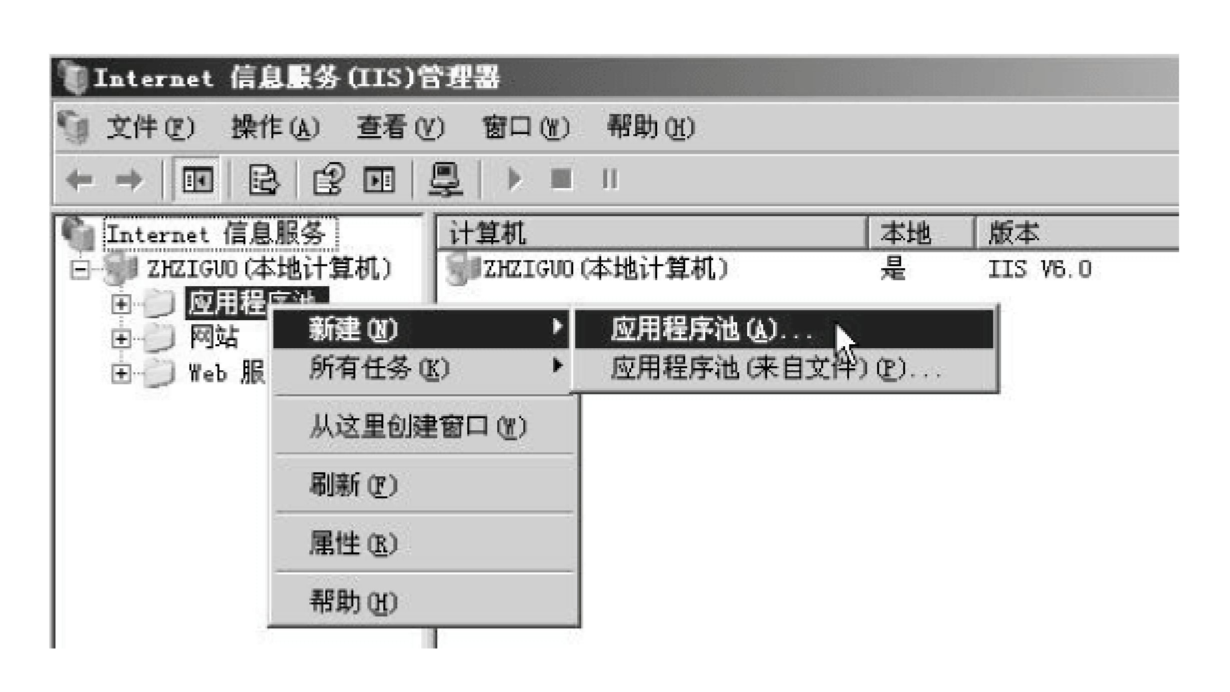


图6-74　新建应用程序池

(2) 此时弹出【添加新应用程序池】对话框，如图6-75所示。这里在【应用程序池ID】文本框中输入WebMail，然后单击【确定】按钮完成设置。

(3) 此时在图6-74所示窗口左侧树状列表的【应用程序池】路径下就会出现WebMail分支。选择该分支，右击，在弹出的快捷菜单中选择【属性】命令，如图6-76所示。



图6-75　【添加新应用程序池】对话框

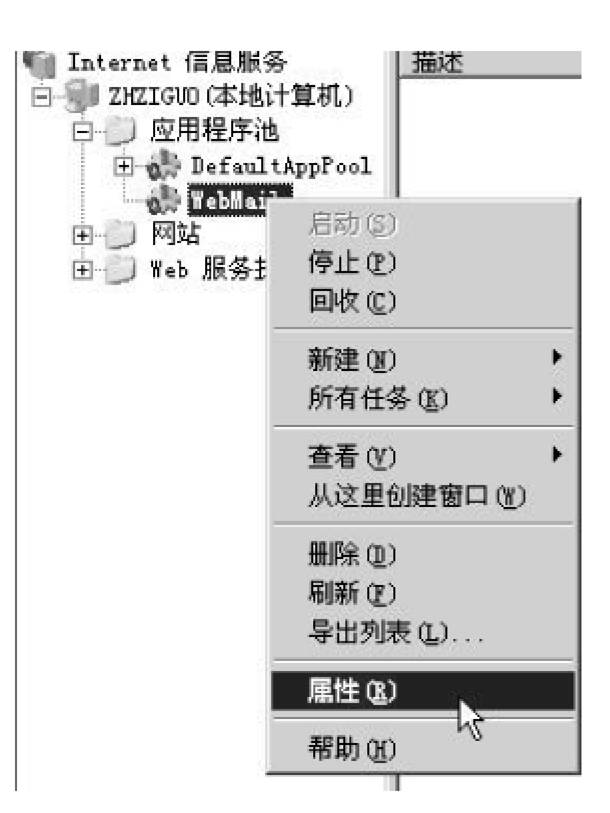


图6-76　查看应用程序池属性



(4) 此时弹出【WebMail 属性】对话框。首先选择【性能】选项卡,取消选中【空闲超时】和【请求队列限制】选项区域中的两个复选框,如图 6-77 所示。

(5) 接着选择【标识】选项卡。在该选项卡中首先选中【预定义账户】单选按钮,然后将【预定义账户】列表框内容更改为“本地系统”,如图 6-78 所示。单击【确定】按钮。



图 6-77 【WebMail 属性】对话框—【性能】选项卡



图 6-78 【WebMail 属性】对话框—【标识】选项卡

(6) 此时弹出【IIS 管理器】对话框。单击【是】按钮完成配置,如图 6-79 所示。

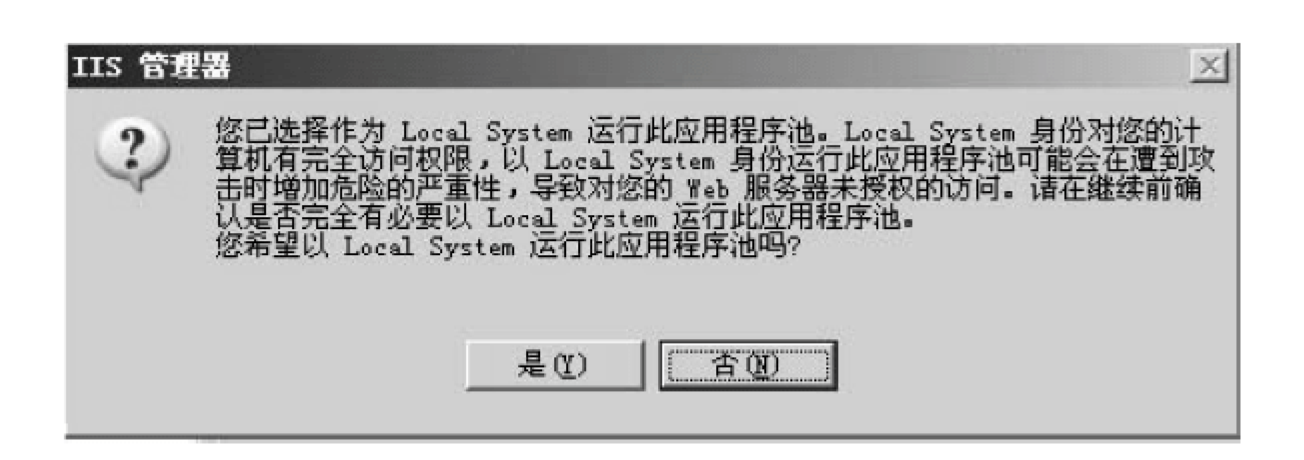


图 6-79 【IIS 管理器】对话框

(7) 新建网站。同样,在【Internet 信息服务(IIS)管理器】窗口左侧树状列表中选择【网站】,右击,在弹出的快捷菜单中依次选择【新建】→【网站】命令,会弹出【网站创建向导】对话框。此时单击【下一步】按钮,会进入网站描述界面,如图 6-80 所示。这里输入网站描述为 WorldClient,单击【下一步】按钮继续。

(8) 此时会进入 IP 地址和端口设置界面,如图 6-81 所示。这里在【网站 IP 地址】列表框中选择服务器地址 192.168.1.11,在【网站 TCP 端口】文本框中输入 80,在【此网站的主机头】文本框中输入用户注册的邮件服务器的域名,这里采用默认值“无”。单击【下一步】按钮继续。

(9) 此时会进入网站主目录界面,如图 6-82 所示。这里可以在【路径】文本框中直接输入 D:\MDaemon\WorldClient\HTML,或者单击右侧的【浏览】按钮在弹出的【浏览文件夹】对话框中选择对应目录,单击【下一步】按钮继续。





图 6-80　【网站创建向导】对话框—网站描述

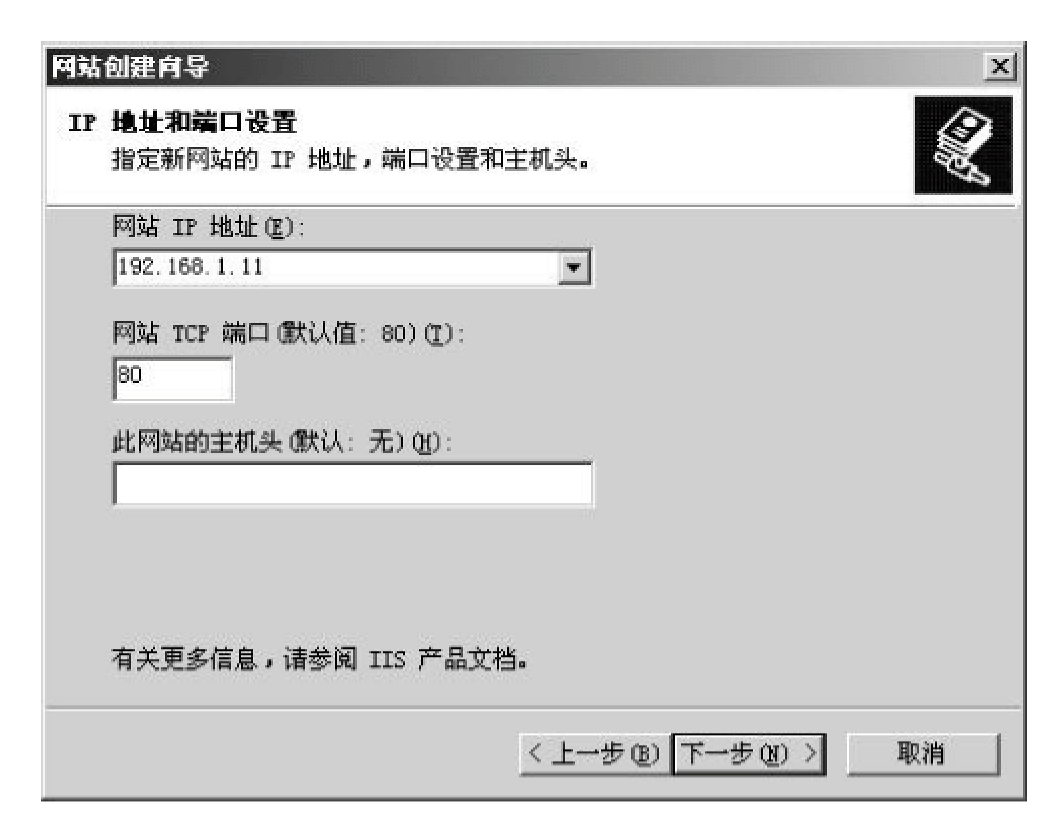


图 6-81　【网站创建向导】对话框—IP 地址和端口设置

(10) 此时会进入网站访问权限界面，如图 6-83 所示。这里依次选中【读取】、【运行脚本】和【执行】三个复选框，单击【下一步】按钮，在弹出的界面中单击【完成】按钮完成网站的创建。



图 6-82　【网站创建向导】对话框—网站主目录

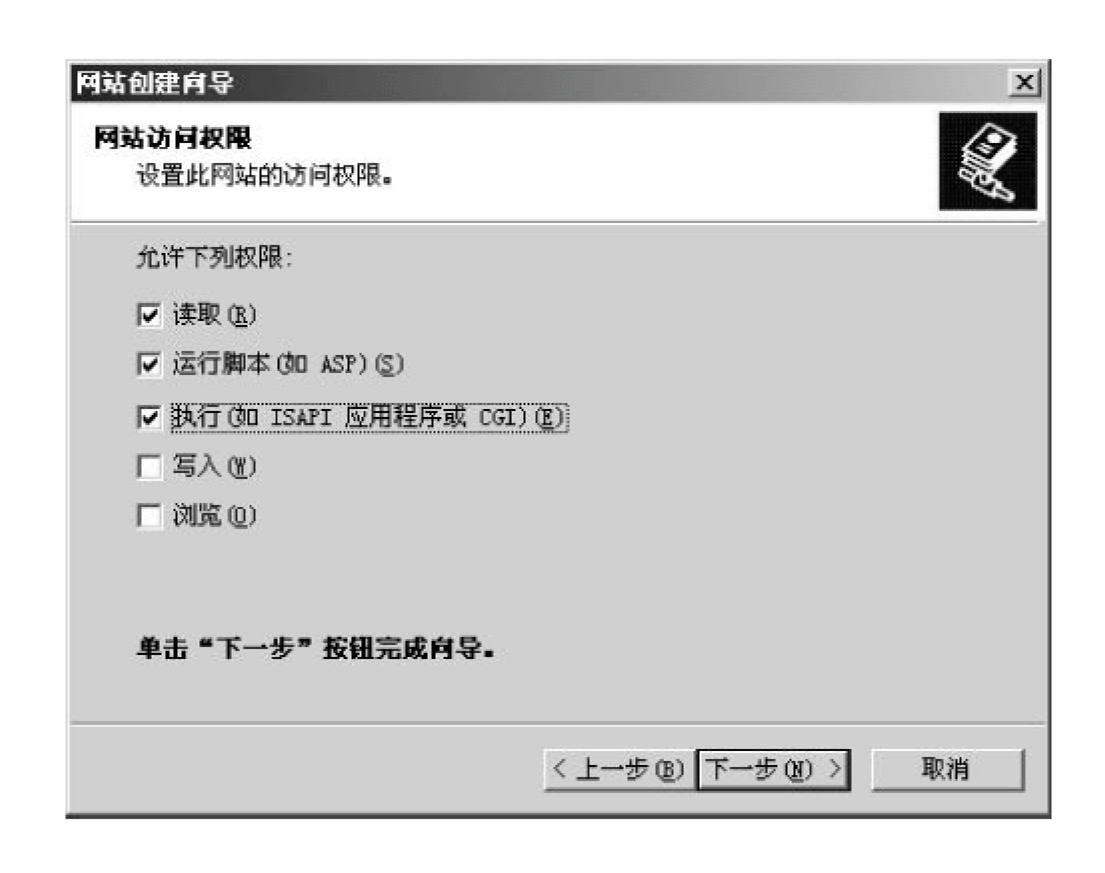


图 6-83　【网站创建向导】对话框—网站访问权限

(11) 此时在图 6-74 所示窗口左侧树状列表的【网站】路径下就会出现 WorldClient 分支。选择该分支，右击，在弹出的快捷菜单中选择【属性】命令，会弹出【WorldClient 属性】对话框。首先选择【主目录】选项卡，在下方的【应用程序池】列表框中选择 WebMail(就是之前建立的那个池)，如图 6-84 所示。

(12) 接着选择【文档】选项卡。在该选项卡中首先单击【启用默认内容文档】选项区域中的【添加】按钮，在弹出的【添加内容页】对话框中输入 WorldClient 的运行文件 worldclient.dll，这样网站的默认首页就是 WorldClient 的运行文件了。然后再单击【启用默认内容文档】选项区域中的【上移】按钮，将 worldclient.dll 移动到第一位，如图 6-85 所示。这样 IIS 默认运行的第一个文档就是 worldclient.dll。单击【确定】按钮完成设置。





图 6-84 【WorldClient 属性】对话框—【主目录】选项卡

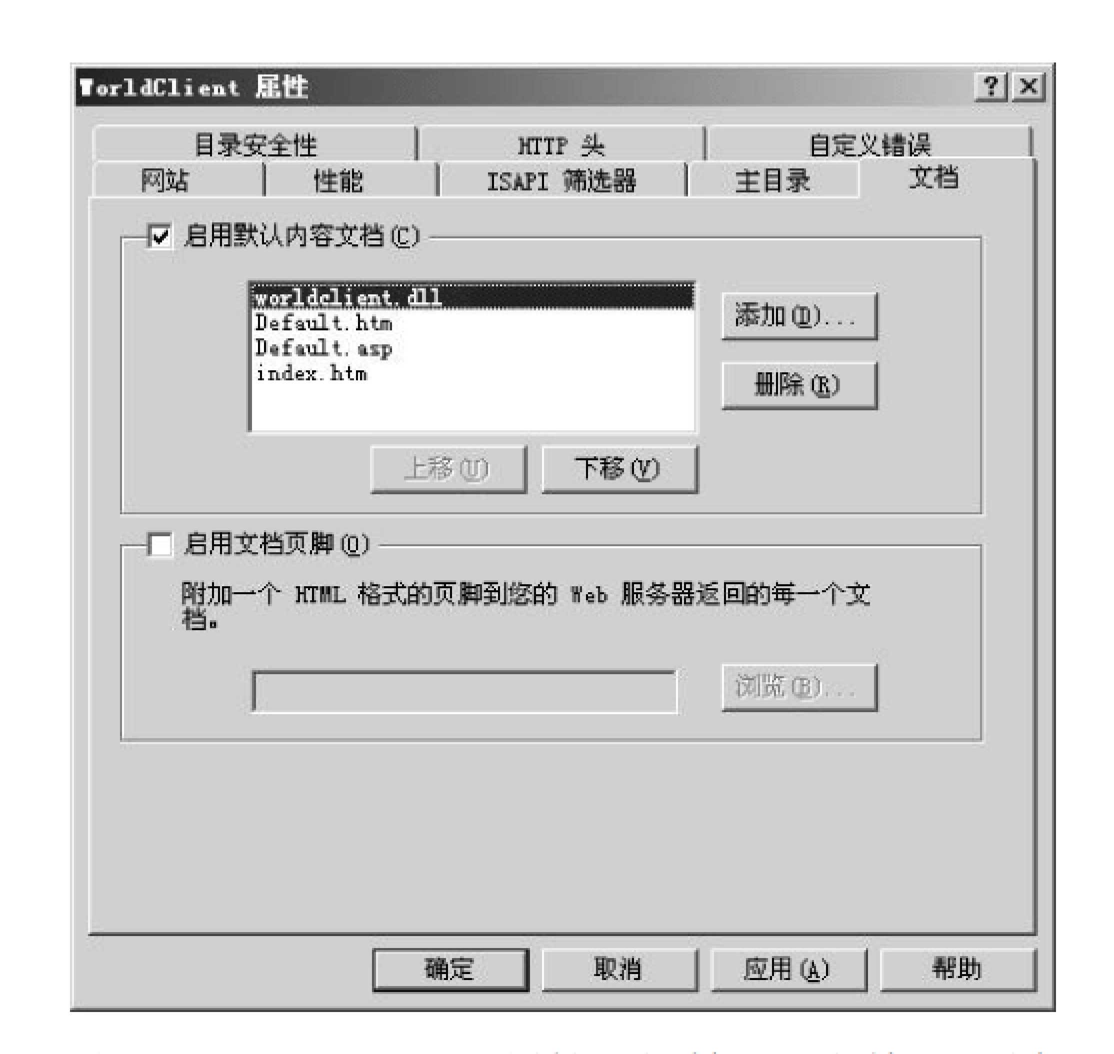


图 6-85 【WorldClient 属性】对话框—【文档】选项卡

(13) 再次在图 6-74 所示窗口左侧树状列表的【网站】路径下选择 WorldClient 分支，右击，在弹出的快捷菜单中选择【权限】命令，会弹出网站主目录路径 D:\MDaemon\WorldClient\HTML 安全设置对话框。在该对话框中首先单击【添加】按钮，会弹出【选择用户或组】对话框。此时在【输入对象名称来选择】文本框中添加 Everyone 账户和启动 IIS 进程账户(IWAM 账户，具体名称根据计算机名称设置有所不同，此处为 ZHZIGUO\IWAM_ZHZIGUO)，如图 6-86 所示。单击【确定】按钮返回网站主目录路径 D:\MDaemon\WorldClient\HTML 安全设置对话框。

(14) 在上方的【组或用户名称】列表框中依次选择上一步添加的两个账户，在下方的【启动 IIS 进程账户的权限】中选中【完全控制】复选框，如图 6-87 所示。最后单击【确定】按钮完成设置。



图 6-86 【选择用户或组】对话框

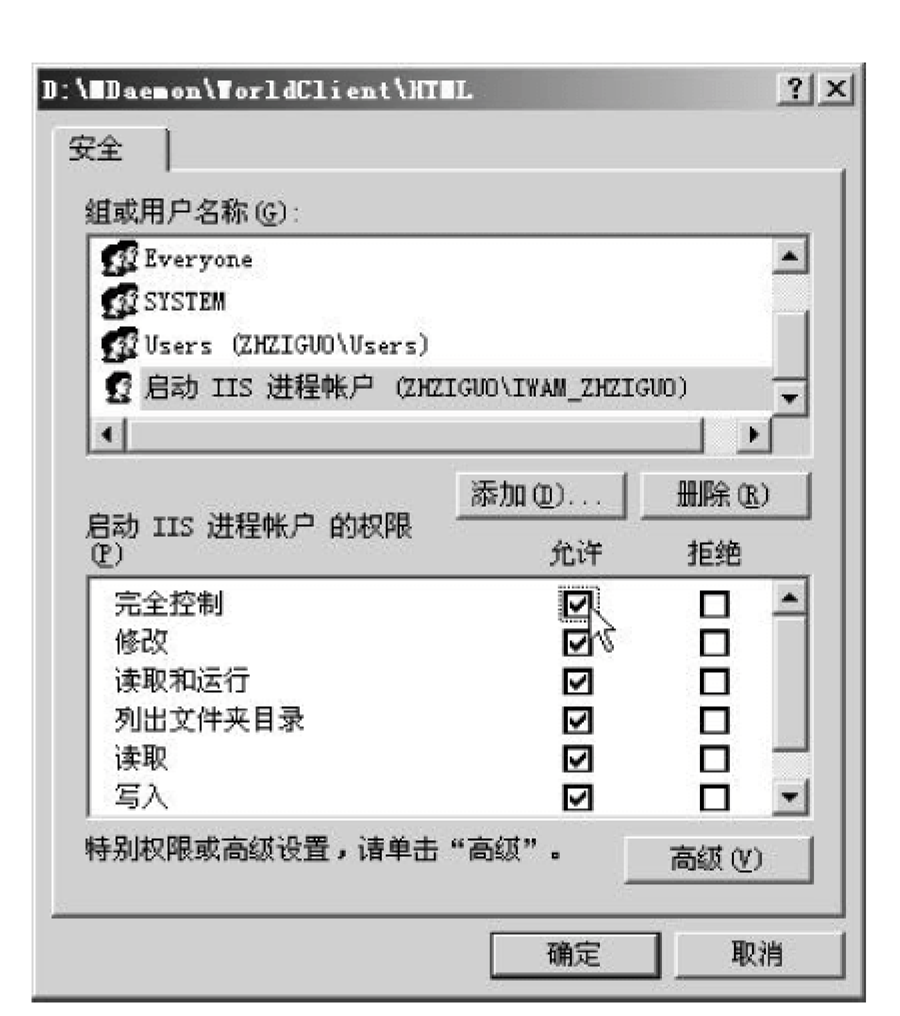


图 6-87 D:\MDaemon\WorldClient\HTML 安全设置对话框



(15) 在【Internet 信息服务(IIS)管理器】窗口左侧树状列表中选择【Web 服务扩展】选项，在右侧选择【所有未知 ISAPI 扩展】，其初始状态是“禁止”，此时在中间位置选择【允许】命令，在弹出的【IIS 管理器】对话框中单击【是】按钮完成设置。此时 Web 服务扩展状况如图 6-88 所示，这样 worldclient.dll 才能被 IIS 执行。

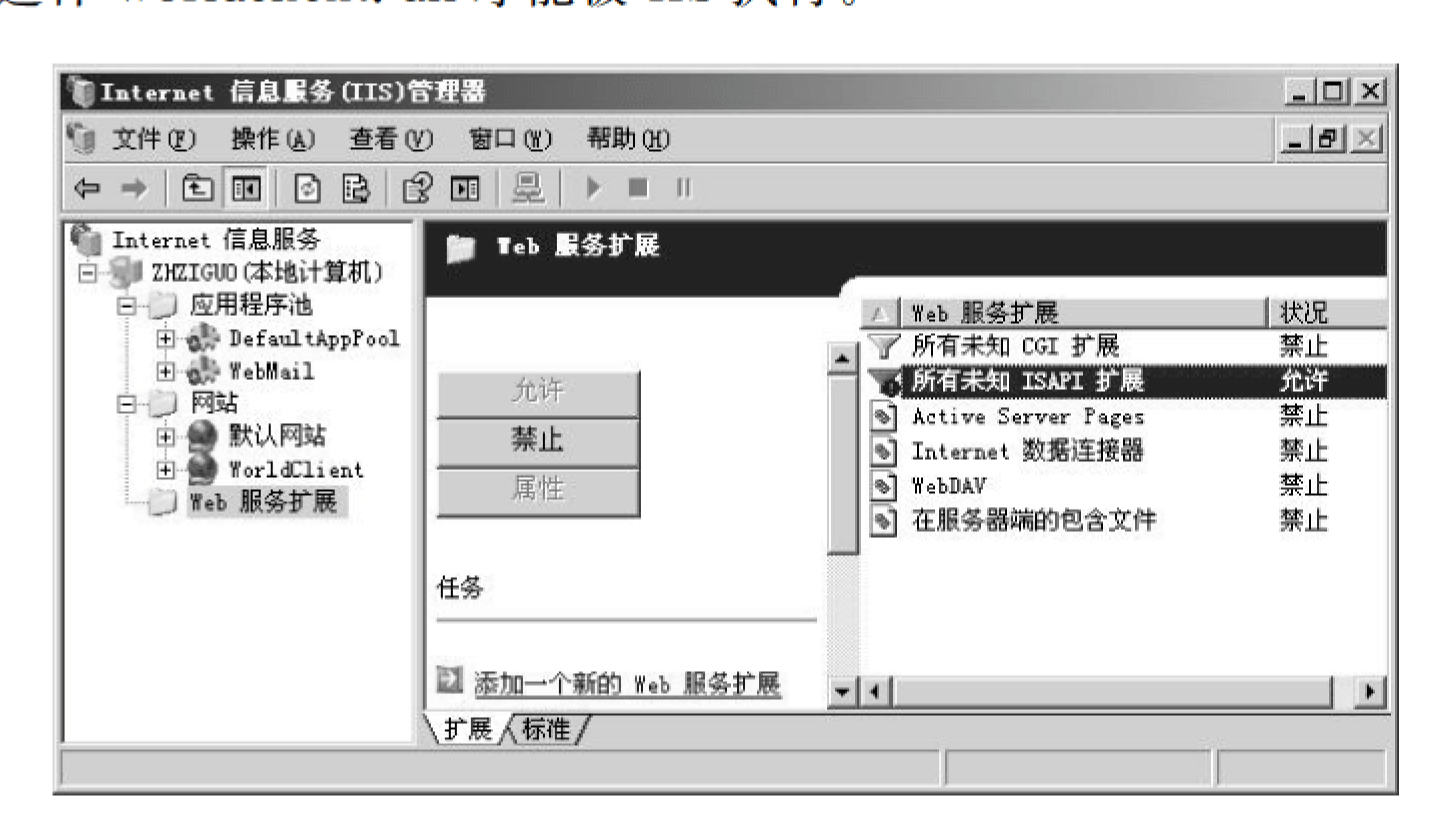


图 6-88　【Web 服务扩展】设置

(16) 设定 WorldClient 运行于 IIS 中。在 MDaemon 的主界面中依次选择【设置】→【Web 及 SyncML 服务】，会弹出如图 6-33 所示的【WorldClient(web 邮件)】对话框。首先在该对话框右侧的【WorldClient(web 邮件)】选项区域中，选中【WorldClient 使用外部 web 服务器运行(IIS、Apache 等)】单选按钮，然后单击下方的【重启 WorldClient】按钮，重新启动 WorldClient，最后单击【确定】按钮完成设置。

(17) 在浏览器中测试。打开 IE 浏览器，在地址栏中输入 http://192.168.1.11，按 Enter 键后界面如图 6-89 所示，表明配置正确完成。



图 6-89　在浏览器中测试



提示：与 WorldClient 一样，WebAdmin 也支持以自服务方式和其他 ISAPI 方式运行，而且二者配置步骤也非常类似，不过 WebAdmin 的配置方法比 WorldClient 略易，具体步骤不再赘述。

6.6 疑难解答

(1) 如果收发邮件的时候出现"超时"错误该如何解决？

选择【设置】→【默认域/服务器】→【超时】命令，在弹出的对话框中进行以下设置：

- 等候 60s 后放弃套接字连接。
- 等候 60s 至协议对话框启动，失败后再放弃。
- 等候 45s 至服务器响应。
- 等候 45s 至 A 记录 DNS 服务器响应。
- 设置等待时间为 250ms。

(2) 安装 MDaemon 时提示"数据执行保护"，该如何设置？

这种情况一般出现在图 6-9 所示界面中。为系统安全起见选取了【除所选之外，为所有程序和服务启用数据执行保护】单选按钮时，单击下方的【添加】按钮，输入以下需要排除保护的进程即可：

- \MDaemon\app\MDaemon. exe
- \MDaemon\app\CFEngine. exe
- \MDaemon\SpamAssassin\MDSpamD. exe
- \MDaemon\WorldClient\WorldClient. exe
- \MDaemon\WebAdmin\WebAdmin. exe
- \MDaemon\SecurityPlus\ScanningProcess. exe (will only be present if you have installed a version of SecurityPlus prior to 4. 00)

另外，当 MDaemon 进行覆盖安装，或者全新安装的时候都必须要重新进行排除一次。

(3) MDaemon 提示磁盘空间不足，有哪些文件可以进行清理？

可以清理以下文件以释放磁盘空间：

① 旧的日志(MDaemon\logs)

② 旧的配置文件(MDaemon\Backup)

③ 坏队列(MDaemon\Queues\Bad)

④ 贝叶斯学习文件夹(MDaemon\Public Folders\Bayesian Learning. IMAP)下的 Non-Spam. IMAP 和 Spam. IMAP 两个文件夹中的内容。

另外，建议在服务器启用初期，做好以下设置：

① 限制邮箱账户的容量，选择【账号编辑器】→【配额】命令，在弹出的对话框中进行设置。

② 进行邮件的修剪，选择【设置】→【主域(默认域与服务器)】→【修剪】命令，在弹出的对话框中进行设置。

在邮件清理前应事先告知用户，让其自行将重要邮件及时保存到本地。



(4) MDaemon 的每个文件夹最多能否容纳多少邮件?

根据 MDaemon 现有的命名模式,最多能够容纳 999 999 999 个邮件文件同时存放在队列或者文件夹中。当然,这个数量也受到操作系统以及文件系统的限制。这些限制会使得真正能够存放的邮件数量小于理论数值。

(5) MDaemon 能否修改欢迎邮件的标题?

选择【设置】→【首选项】→【系统】命令,在弹出的对话框中通过修改【新账户"欢迎邮件"主题文本】文本框中的内容来修改欢迎邮件的标题。

(6) MDaemon 能否修改欢迎邮件的内容?

直接修改 MDaemon\app\welcome.dat 文件即可(可以用任意文本编辑器打开该文件)。

另外,在修改时建议暂停 MDaemon 的使用。

习　题

1. 填空题

(1) 电子邮件系统主要由________、________、________三个部分组成。

(2) 电子邮件系统中使用的通信协议主要有三个,分别是________、________和________。

2. 选择题

(1) 常见的邮件传送代理(MTA)程序包括(　　)。

A. Outlook Express　　B. Foxmail　　C. MDaemon　　D. Exchange

(2) MDaemon 的 Web 远程管理功能插件 WebAdmin 依据登录用户级别的不同,提供不同的远程管理功能。其访问级别分为(　　)。

A. 全局管理员　　B. 域管理员　　C. 用户　　D. Guest

3. 思考题

(1) MDaemon 常用的插件有哪些? 各自的作用是什么?

(2) 运行 WorldClient 有哪两种方式? 二者的区别是什么?

4. 上机题

(1) 在服务器端进行设置,关闭 MDaemon 默认的强密码要求。

(2) 使用浏览器,在远程创建一个名为 chapter6test 的邮箱账户。



第7章　新闻服务

本章要点

- 新闻组服务器和客户端的工作原理
- DNews 新闻服务器的安装、配置和管理

新闻服务也称为新闻组服务，曾经是 Internet 上与 WWW、E-mail 与 FTP 齐名的四大网络信息服务系统之一，其对应的英文名称是 NewsGroup。目前在国外，新闻组的使用仍然十分广泛，但由于种种原因，国内的新闻服务器数量相对较少。

7.1　新闻服务概述

新闻组最早出现于 1980 年美国北卡罗来纳州。它是一个基于网络的计算机的组合，这些计算机就是新闻服务器。简单地说，新闻组是一个可以离线浏览的论坛，在线时可以把新闻组里面的帖子先接收到自己的计算机中，断线后仍旧可以阅读。新闻组用户通过新闻组客户端软件就可以连接到新闻服务器上，下载阅读其他人发上去的帖子并可以进行回复和讨论。它和现在使用的论坛差不多，不过它是不需要进行注册的，是任何一个网络用户都能进行相互交流的平台。新闻组服务器与客户端程序是采用网络新闻传送协议（Network News Transfer Protocol，NNTP），使用的端口号是 119。

新闻组是一种高效而实用的工具，它具有四大优点：

- 海量信息。据有关资料介绍，目前国外有新闻服务器 5000 多个，最大的新闻服务器包含 39 000 多个新闻组，每个新闻组中又有上千个讨论主题，其信息量之大难以想象，就连 WWW 服务也难以相比。
- 直接交互性。在新闻组上，每个人都可以自由发布自己的消息，不管是哪类问题、多大的问题，都可直接发布到新闻组上和成千上万的人进行讨论。这似乎和 BBS 差不多，但它比 BBS 有两大优势，一是可以发表带有附件的“帖子”（随着时代的发展，现在 BBS 也可以传附件了），传递各种格式的文件；二是新闻组可以离线浏览。但新闻组不提供 BBS 支持的即时聊天，也许这就是新闻组在国内使用不广的原因之一。
- 全球互联性。全球绝大多数的新闻服务器都连接在一起，就像互联网本身一样。在某个新闻服务器上发表的消息会被送到与该新闻服务器相连接的其他服务器上，每

一篇文章都可能漫游到世界各地。这是新闻组的最大优势，也是网络提供的其他服务项目所无法比拟的。

- 主题鲜明。每个新闻组只要看它的命名就能清楚它的主题，所以在使用新闻组时其主题更加明确，往往能够一步到位，而且新闻组的数据传输速度与网页相比要快得多。

7.1.1　新闻服务基础知识

1. 新闻组的起源

新闻组是由世界范围的计算机组成的共享新闻和邮件的国际化网络。新闻组的英文名称为 Usenet 或 NewsGroup，起源于美国北卡罗来纳州。1980 年，两个学生(Tom Trusctt 和 James Ellis)在几台 UNIX 计算机上生成第一版 Usenet，它能在一天之内通过一种被称为 UUCP(UNIX-to-UNIX Copy)的网络协议，将大批文章从一台计算机传到另一台计算机上。几年之内，这种 Usenet 的改良版本被推广到了其他几所大学和几家软件公司之中。接下来的几年里，Usenet 得到迅猛传播，其信息量也从 1983 年的每天几百篇文章增加到现在的每天几万条，其主题已经涵盖了人类社会所能涉及的所有内容，如科学技术、人文社会、地理历史、休闲娱乐等。无论用户有什么样的问题，都可以发送到新闻组上，届时会有成千上万的人一起讨论这一问题，帮助用户找到最好的解决方法。新闻组最初的方向是用于支持计算机方面的疑问与解答，但是到了 20 世纪 80 年代后期，不同的新闻组，也就是讨论方向，已经发展到了将近 1000 个。

2. 与其他网络应用的对比

新闻组的实时性没有论坛好，但是客户端不必登录到服务器，安全性相对要好。另外，新闻组可以离线浏览，这在论坛中是不可能的。与电子邮件相比，电子邮件保存在客户端，只有收件人能够查看和保存，而新闻组存储在服务器端，可以随时查阅。与文档相比，新闻组的优越性在于时效性和便于沟通，文档的优越性在于条理性和归档保存。每个新闻组都具有鲜明的主题。这和 Web 不同，虽然 Web 的网页做得越来越精致、越来越美观，但大多数时间只是从一个页面转到另一个页面，漫无头绪，而且由于图片、广告条的影响，Web 的传输速度太慢。而新闻组则不同，每个新闻组只要看它的命名就能清楚它的主题，所以在使用新闻组时其主题更加明确，往往能够一步到位，而且新闻组的数据传输速度与网页相比则要快许多。

3. 新闻组的组成结构

新闻组服客户端程序是按分类组织各个新闻分组的，接收由用户直接发送到服务器上的帖子，发送的帖子可以带有背景图案或音频，还可以附加各类文档、程序，以及图形、图像和多媒体内容等。新闻组还可以周期性地与相邻的其他新闻组服务器交换内容，采用这种接力传送的方法就可以获得各个新闻组服务器上的内容，再将所获得的内容定期保存于相应的新闻分组中，过期的帖子则由系统自动删除掉。NNTP 需要设置一台或多台中心新闻



服务器,用来保留所有的新闻文章,服务器端可以设置不同的新闻组对新闻信息加以分类,用户端根据所订阅的新闻组与服务器端进行数据同步,接收到的稿件根据新闻组的分类规则对所属信息进行层次化展示,便于信息查找。打开新闻组服务器将允许发/读任何人的帖子,访问被限制的新闻组服务器,匿名发帖或发送 SPAM。

新闻组的组成结构呈树状等级结构,通常是根据讨论的主题或类型分类的。例如,Linux 新闻组通常被安排在 alt. os、comp. os. linux 或者 Linux 主题下。可以看出,关于 Linux 操作系统的一些诸如设置、硬件或者 X. 11 等讨论问题都被安排在计算机—操作系统—Linux 的主题下。许多其他的讨论问题也是按照这个方法组织安排的,这样在大多数情况下就可以很容易地找到一个讨论感兴趣的问题的新闻组。

目前已经有几十种不同的新闻组客户端软件、传输程序和新闻阅读器程序,还有超过十万个不同的新闻组。所有新闻阅读器程序都能够提供下列基本的功能:

- 订阅或停止订阅某个新闻组。
- 浏览消息并阅读后续消息(线索)。
- 直接向消息的作者回复一个邮件消息。
- 针对某个新闻组上的消息发布后续评论。
- 保存某个消息的内容(通常保存在用户子目录中名为 News 的子目录中)。

7.1.2 新闻组服务器和客户端的工作原理

1. 新闻发布流程

新闻发布流程如图 7-1 所示。

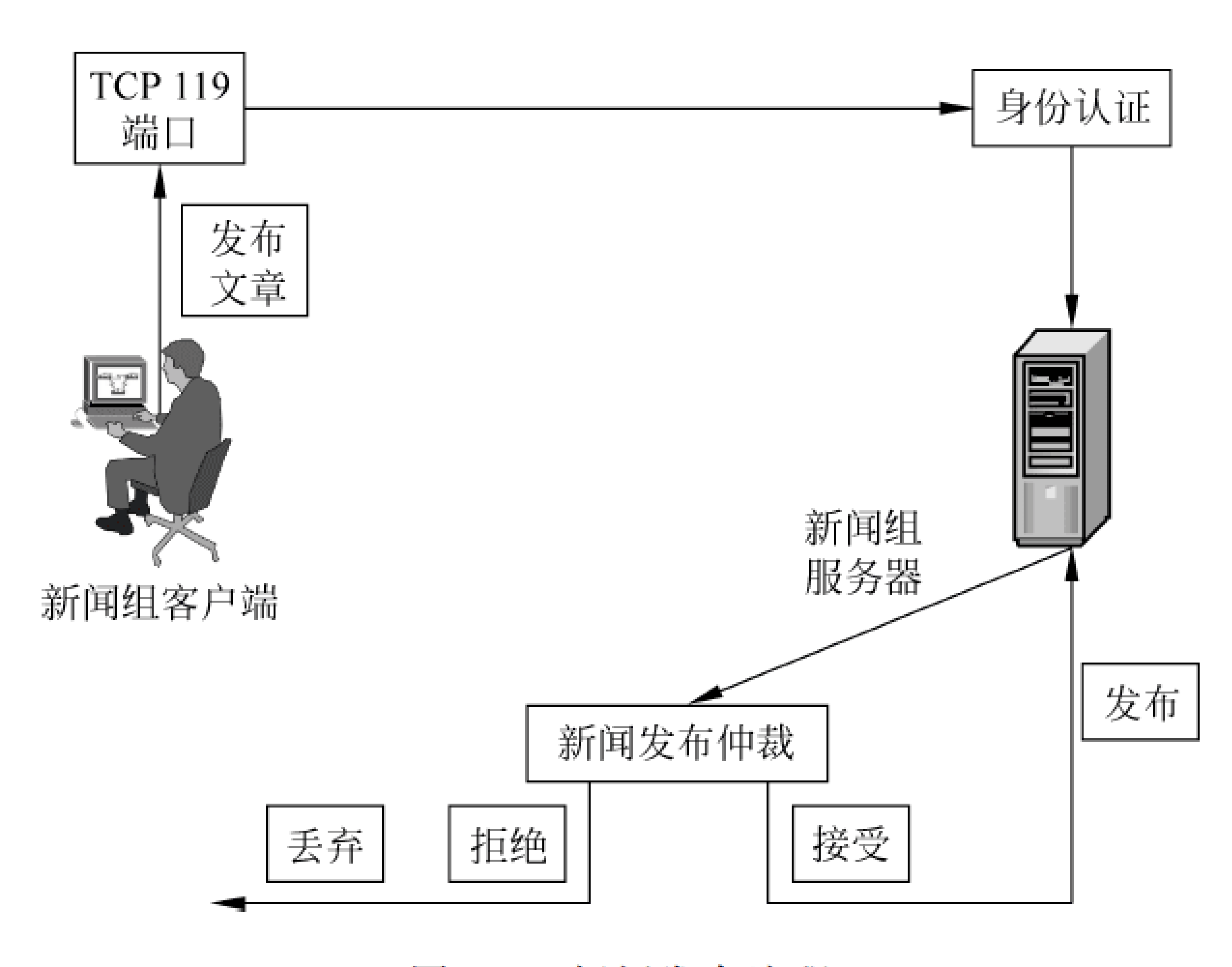


图 7-1 新闻发布流程

(1) 客户端使用新闻组软件通过 TCP 119 端口向新闻组服务器发送请求,要求发布新闻组文章。

(2) 新闻组服务器对客户端用户进行身份认证,确定客户端是否有发布新闻组文章的权限。



(3) 通过身份认证后客户端就可以登录新闻组服务器。

(4) 新闻组服务器的新闻发布控制端检查文章,新闻发布控制端拒绝的文章将被丢弃,新闻发布控制端接受的文章将被发布和存储。

2. 客户端查看新闻组文章流程

客户端查看新闻组文章流程如图 7-2 所示。

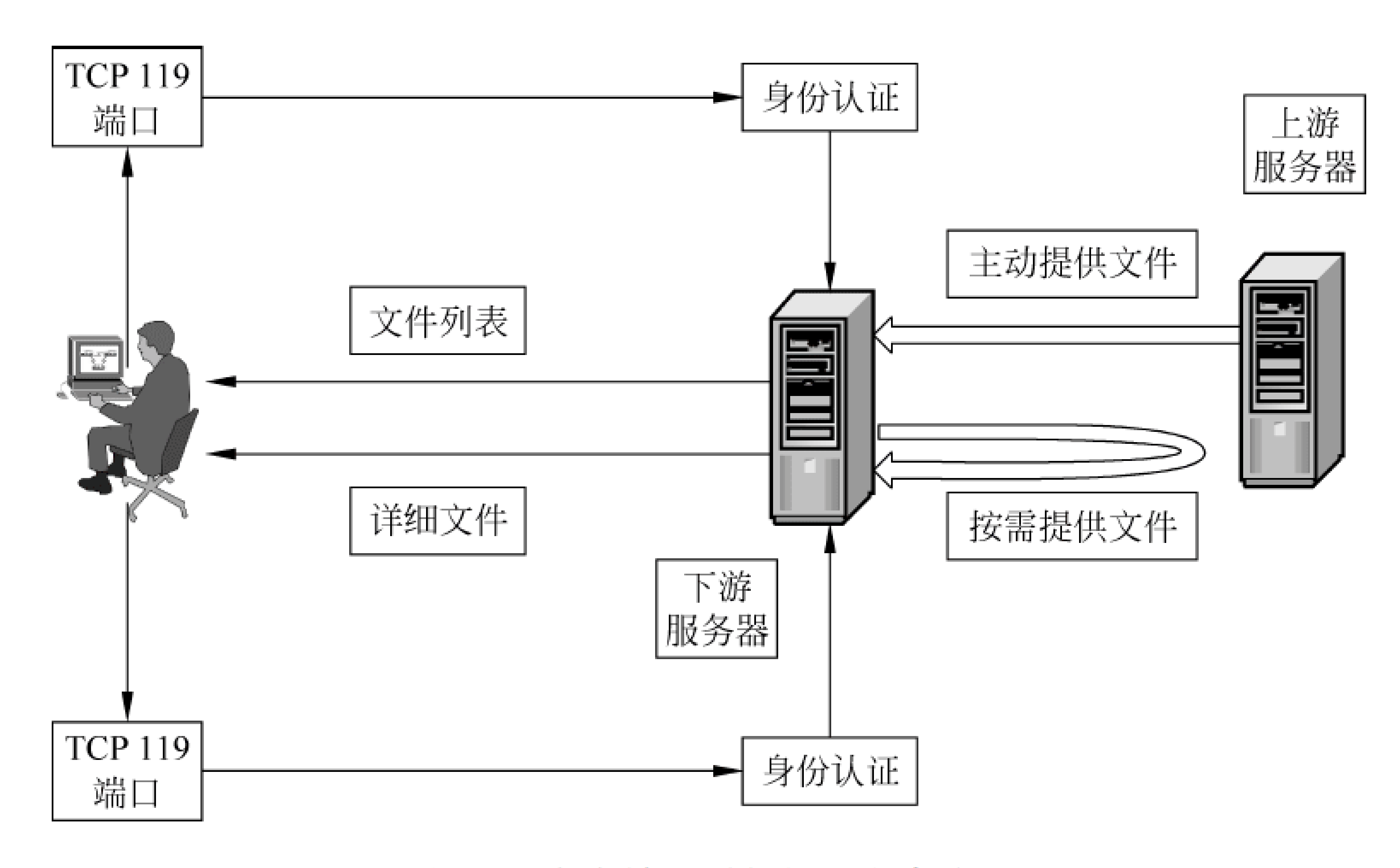


图 7-2　客户端查看新闻组文章流程

(1) 客户端使用新闻组软件(浏览器等)通过 TCP 119 端口向新闻组服务器发送请求,要求提供新闻组文章列表。

(2) 新闻组服务器对客户端用户进行身份认证,确定客户端是否有阅读新闻组文章列表的权限。

(3) 通过身份认证后客户端就可以登录新闻组服务器。

(4) 新闻组服务器向客户端转送新闻组文章列表。

(5) 客户端再次使用新闻组软件通过 TCP 119 端口向新闻组服务器发送请求,从新闻组文章列表中列出希望查看的文章。

(6) 新闻组服务器对客户端用户进行二次身份认证,确定客户端是否有阅读文章的权限。

(7) 通过身份认证后客户端就可以登录新闻组服务器。

(8) 新闻组服务器向客户端转送允许阅读的新闻组文章。

(9) 另外,下游新闻组服务器和上游新闻组服务器之间文章传递(feed)通常使用主动提供和按需提供两种。

7.2　安装 DNews 服务器

DNews News Server(简称 DNews)是一个功能完整的新闻服务器软件,它具有新闻服务器的所有功能,而且还提供了图形配置界面,简化了新闻服务器的配置和管理。在此基础上,DNews 提供了基于 Web 页面的配置管理方式,管理员可以远程对服务器进行管理和配

置。DNews 是 NetWin 公司的产品，DNews 允许用户从互联网上下载使用，并免费使用 4 周。免费使用期过后，用户必须进行注册或停止使用，对于非赢利大学或学校以及 Linux 版本用户，则可以免费注册使用。DNews 支持的操作系统包括 Windows NT/2000/2003/XP、Linux、Solaris、BSD、AIX、VAX VMS 及 ALPHA VMS 等。

本章以 DNews 5.7e1 for Windows 版本为例进行讲解，DNews 的最新下载版本可以从 http://netwinsite.com/cgi-bin/keycgi.exe? cmd=download&product=dnews 获得。

在 Windows Server 2003 环境下，DNews 5.7e1 的安装步骤如下。

7.2.1 安装准备工作

查看服务器硬件配置：在 Microsoft Windows 平台上安装 DNews 5.7e1 版本时的系统要求如表 7-1 所示。从中可以看出，DNews 对系统软硬件要求还是比较低的，在许多情况下，完全可以使用现有的硬件和操作系统来运行 DNews，避免了额外的硬件投入。

表 7-1 在 Microsoft Windows 平台上安装 DNews5.7e1 版本时的系统要求

组　　件	要　　求
CPU	处理速度为 800MHz 的 Intel Pentium 3(或与之等效的)CPU
RAM	128MB
硬盘空间	350MB(安装时需要额外的 30MB)
推荐操作系统	Windows 2000 Server(Service Pack 4) Windows XP Professional Edition 和 Home Edition(Service Pack 2) Windows Server 2003

7.2.2 DNews 新闻服务器的安装

DNews 新闻服务器的具体安装步骤如下：

(1) 双击运行下载的 DNews 软件包 dnews_57e1_windows.exe 文件，出现安全警告界面，如图 7-3 所示。单击【运行】按钮。

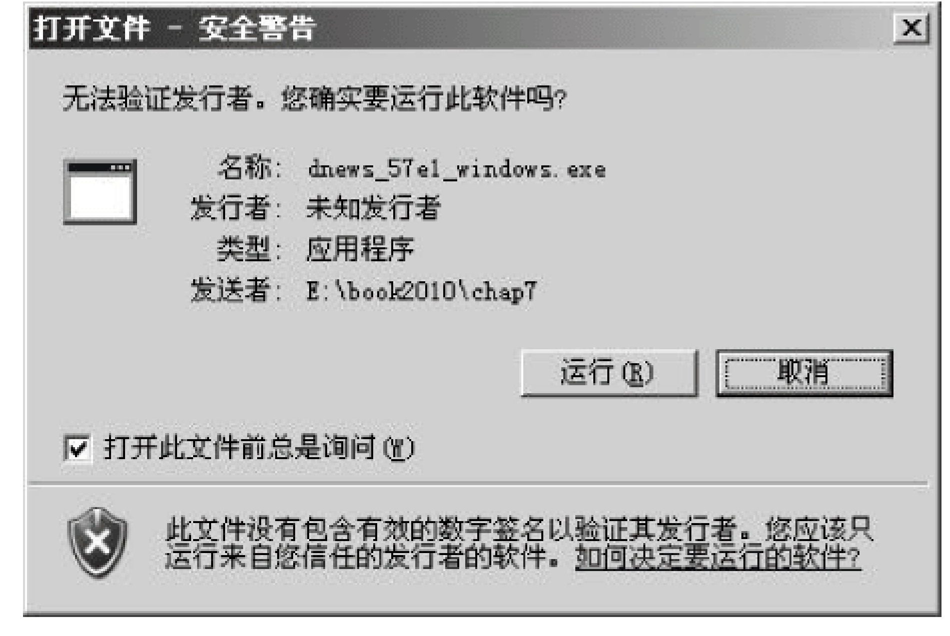


图 7-3 安全警告界面

(2) 出现 DNews Installation /Upgrade 对话框，如图 7-4 所示。DNews 软件包是一个自解压文件，在该对话框中确定解压文件的安装目录。这里采用默认安装目录“\dtemp”，单击 Unzip 按钮。

(3) 软件包开始解压，解压完成后，自动开始安装。此时出现 You may want to reformat your drives 对话框，如图 7-5 所示。为提高磁盘性能，系统会建议格式化 DNews 所要安装的硬盘分区。注意这只是一个建议，真正的格式化操作需要用户手动进行。单击 Continue 按钮继续。

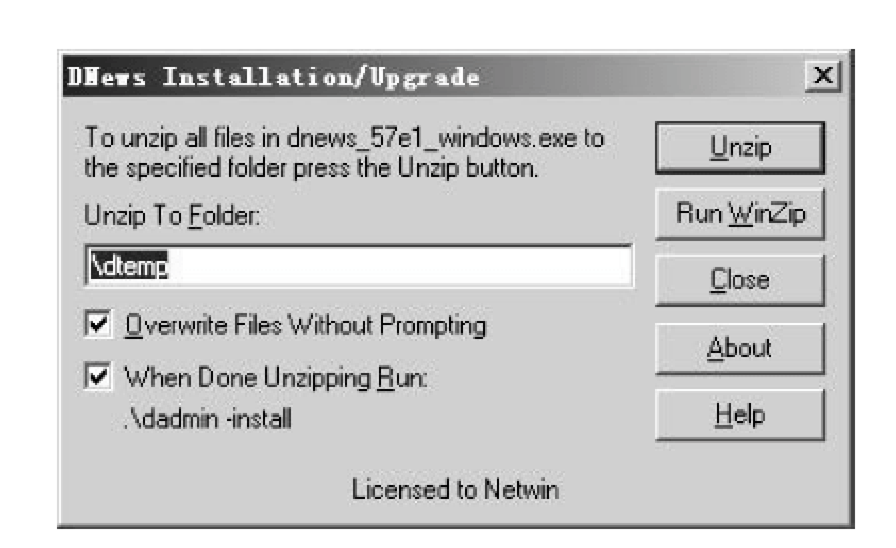


图 7-4　DNews Installation /Upgrade 对话框



图 7-5　You may want to reformat your drives 对话框

(4) 此时出现 Enter “yes” to continue 对话框,如图 7-6 所示。系统询问是否阅读并认可软件许可协议,在 Enter “yes” to continue 文本框中输入 yes,单击 Next 按钮。



图 7-6　Enter “yes” to continue 对话框

(5) 此时出现 DNEWS Setup Wizard(DNEWS 安装向导)对话框,如图 7-7 所示。软件正式开始安装,提示用户首先选择安装类型。可以选择的安装类型及其说明如表 7-2 所示。用户可以根据需要选取,这里选择第一项 Standalone news server, local groups only,单击 Next 按钮。



图 7-7　DNEWS Setup Wizard 对话框



表 7-2　DNews 的安装类型及其说明

安 装 模 式	模式类型	应 用 说 明
Standalone news server, local groups only	单一模式	建立一个本地的新闻组服务器,不参加全球的新闻组的转信,适于小型的新闻组服务器,或者在局域网内部运行。例如中国的新帆、大洋等
Suck/Pull news from another server	转信模式	直接建立一个镜像其他新闻组服务器的新闻组服务器,即参加全球的新闻组的转信,适于中小规模的新闻组服务器。例如中国的希网 cn99 等
Accept traditional push/ihave feed	复合模式	同时允许其他新闻组服务器汲取本地新闻组内容,适于大型的新闻组服务器。例如微软等商业公司

提示：安装完成后,可以设置修改选定的安装类型。例如,可以将单一模式安装的新闻组服务器加入公共新闻组,即设置成转信模式或复合模式。

(6) 此时出现 DNEWS Setup(DNEWS 安装)对话框,如图 7-8 所示。这里需要选择设置一下新闻组的组名命名规则。值得注意的是,只有选择“Allow all groups= * ”才可以建立有中文组名的新闻组,其他选项是不能建立中文新闻组的。这里选择“Allow all groups= * ”,然后单击 Next 按钮。

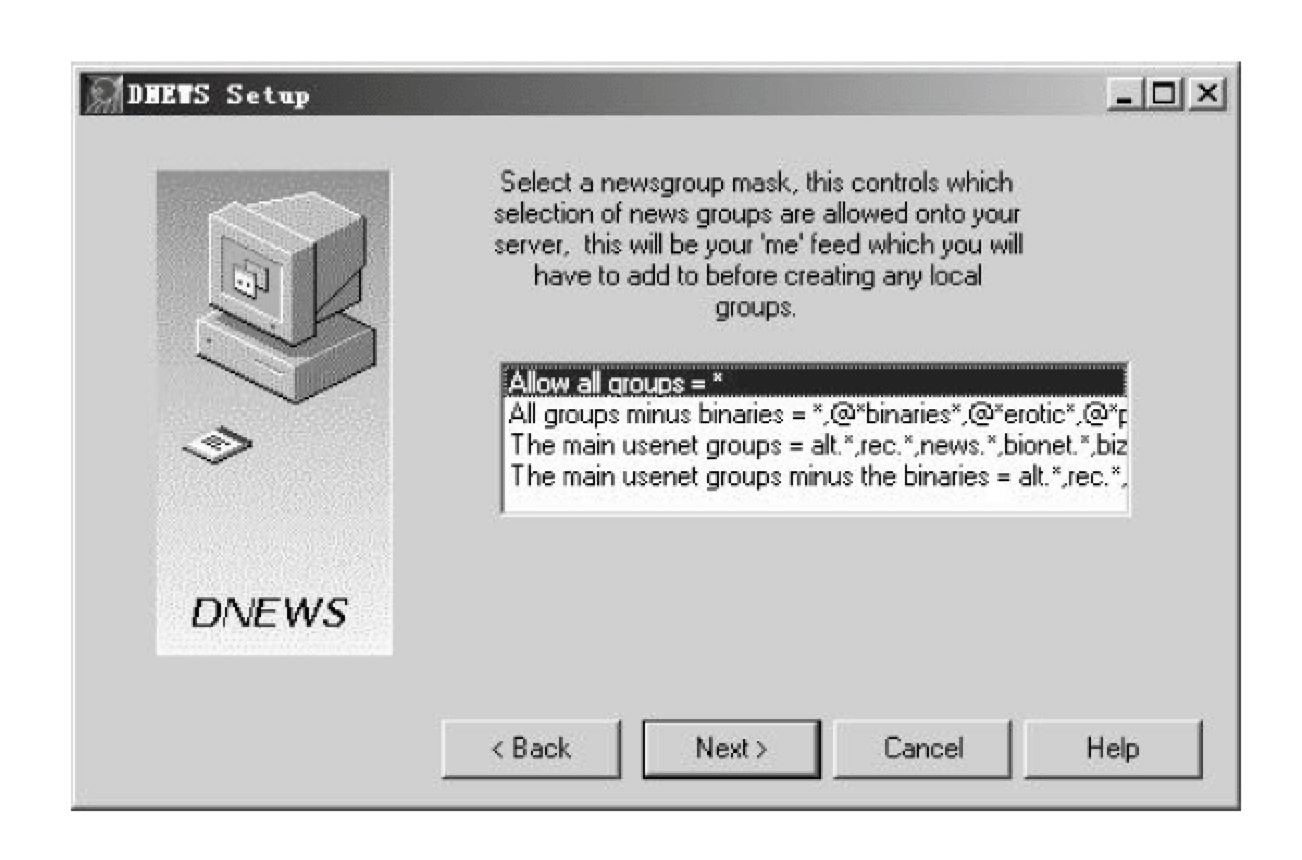


图 7-8　DNEWS Setup 对话框

(7) 此时出现 SMTP host 对话框,如图 7-9 所示。这里需要选择新闻组服务器用于发布帖子的 SMTP 服务器的 IP 地址。在 SMTP host 文本框中填写 SMTP 服务域的 IP 地址,SMTP 服务域用于组织要传递的消息。SMTP 虚拟服务器至少有一个域:默认的本地域。本地域是由本地 SMTP 服务器提供服务的域名系统(DNS)域。到达 SMTP 服务器的包含本地域名的消息或者在本地传送到 Drop 文件夹,或者与不可传递的(NDR)报告一起返回给发送方。这里输入在第 6 章创建的 MDaemon 邮件服务器的 IP 地址 192.168.1.11,然后单击 Next 按钮。

(8) 此时出现 Managers E-mail address(管理员电子邮件地址)对话框,如图 7-10 所示,提示添加新闻组服务器管理员的电子邮件地址。使用该账户可以对 DNews 服务器进行远程设置和管理。在 Managers E-mail address 文本框中填写新闻组服务器管理员的电子邮





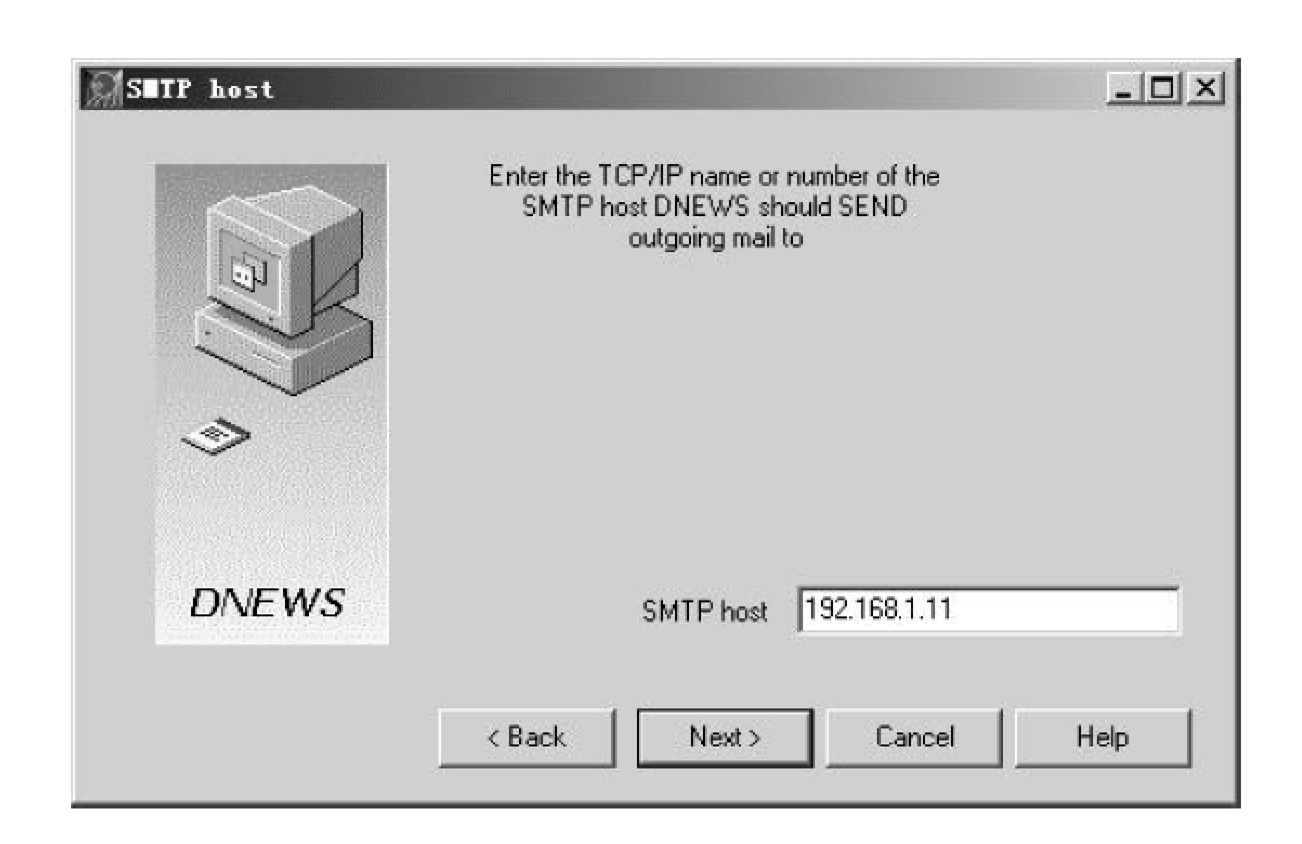


图 7-9 SMTP host 对话框

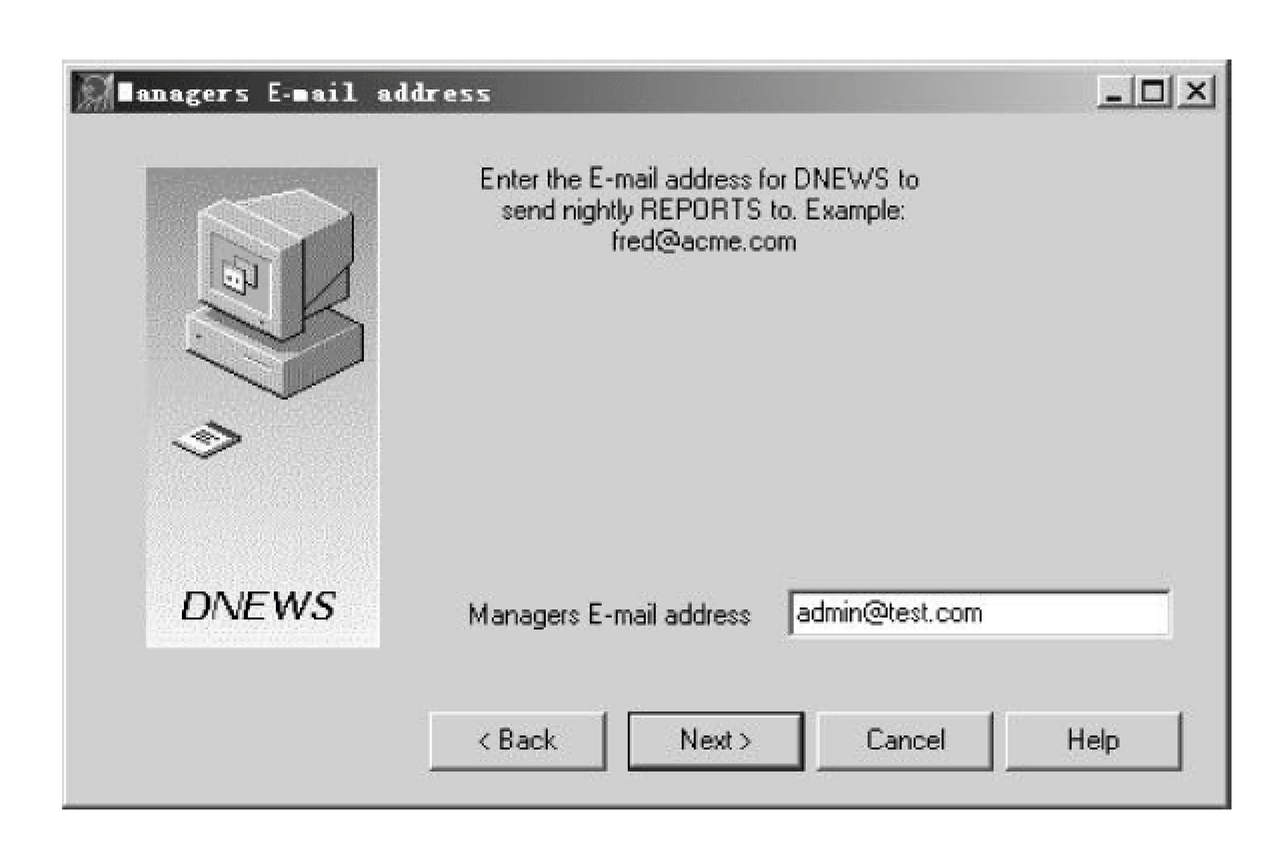


图 7-10 Managers E-mail address 对话框

件地址，如果局域网没有部署邮件系统，也可以直接单击 Next 按钮继续。这里填写在第 6 章创建的邮件服务器管理员 E-mail 地址 admin@test. com，然后单击 Next 按钮。

(9) 此时出现 Allow read/post from 对话框，如图 7-11 所示，提示用户输入允许访问本新闻组服务器的 IP 地址列。这里还可以使用 CIDR 地址(即无类别域间路由选择方案)，顾名思义，它不像有类别机制中那样对地址分类，而是使用最靠前的 k 位定义网络地址，剩下的 32-k 位用于主机地址。这样，一个服务提供商就可以拥有一个这种范围内的网络地址。它的前 14 位是某个固定值(网络地址)，而剩下的 18 位表示了主机部分的地址。这种方法允许服务提供商为客户分配 218 个不同的地址。

根据上面输入的本服务器 IP 地址 192. 168. 1. 11，在此，系统给出的 Allow read/post from 文本框的默认值是 192. 168. 1. *，用户可以更改此值。这里采用该默认值即可，然后单击 Next 按钮。

(10) 此时出现 Allow read/post from 对话框，如图 7-12 所示，提示用户设定可以访问本新闻组服务器的组名。在 Allow read/post from 文本框中输入允许访问本新闻组服务器的本地用户群，这里选择默认值“ * . ”。也就是说，所有本地用户均可以访问本新闻服务器，然后单击 Next 按钮。



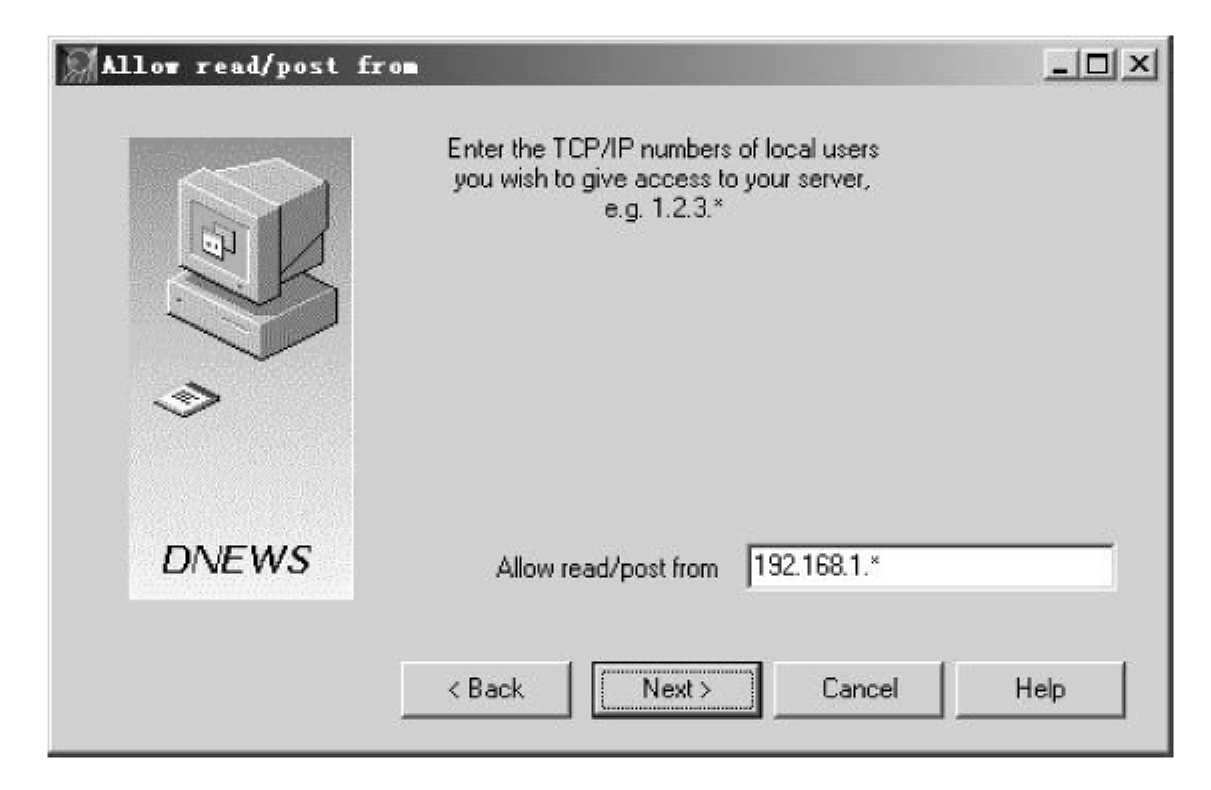


图 7-11　Allow read/post from 对话框—IP 地址

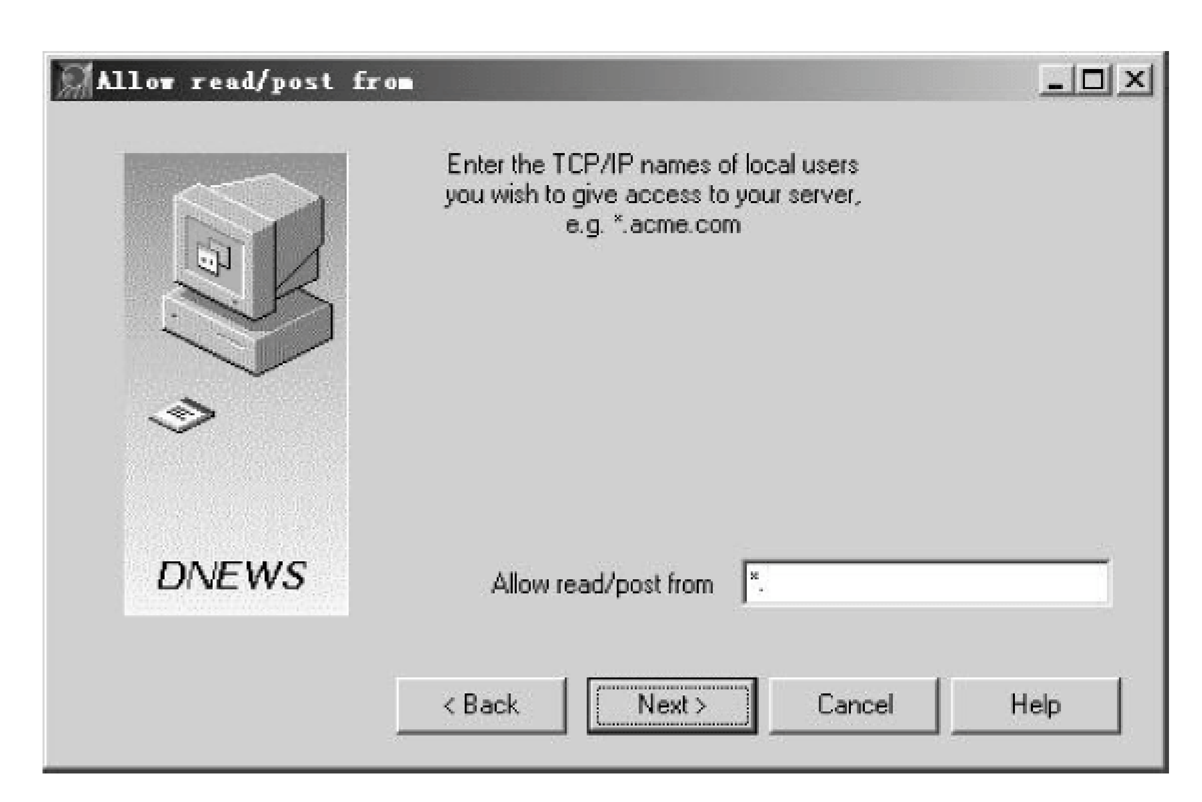


图 7-12　Allow read/post from 对话框—组名

（11）此时出现 Destination CONFIG files 对话框，如图 7-13 所示，提示用户输入 DNews 配置文件的存放位置，即新闻组服务器的安装分区和目录。推荐把 DNews 安装到一个单独的大容量 NTFS 格式分区，这里在 Destination CONFIG files 文本框中输入 D:\dnews，然后单击 Next 按钮。

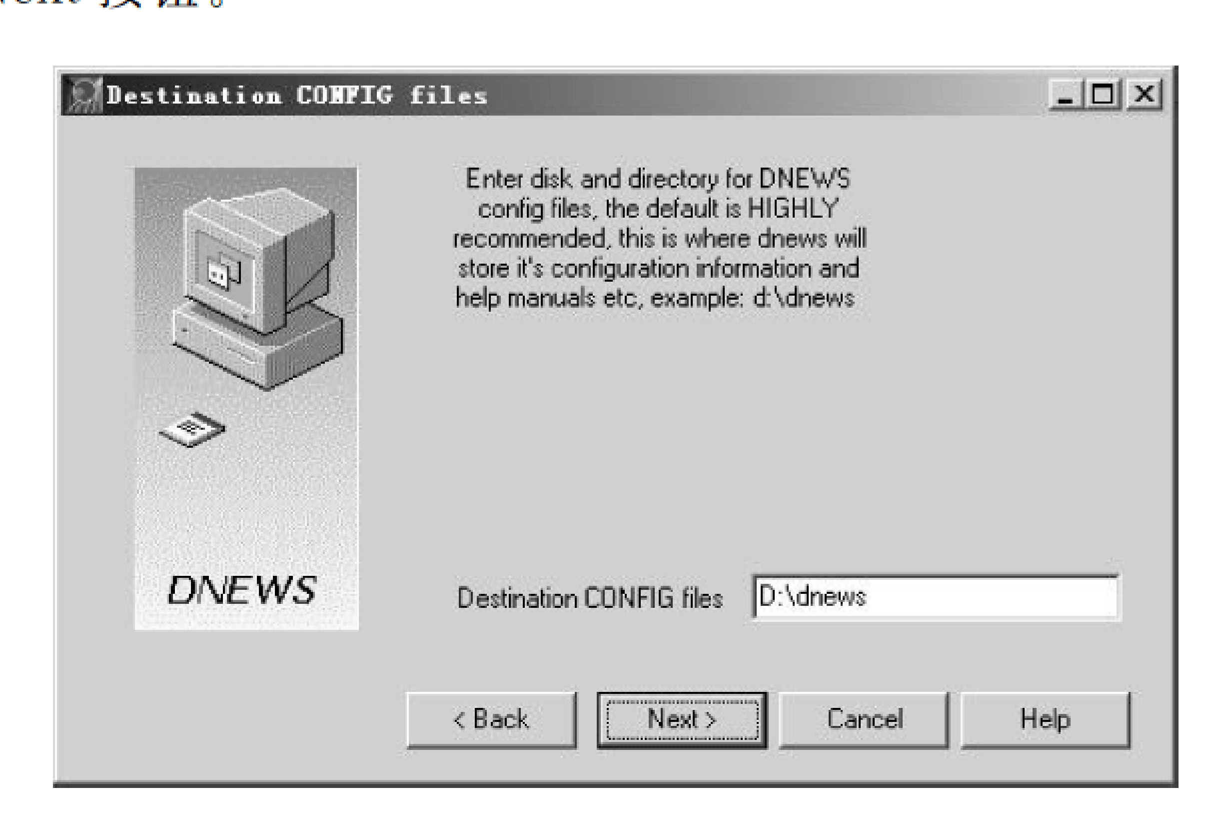


图 7-13　Destination CONFIG files 对话框

（12）此时出现 Destination SPOOL files 对话框，如图 7-14 所示，提示用户输入 SPOOL 文件的存放位置，即设定缓存文件目录。这里在 Destination SPOOL files 文本框中输入



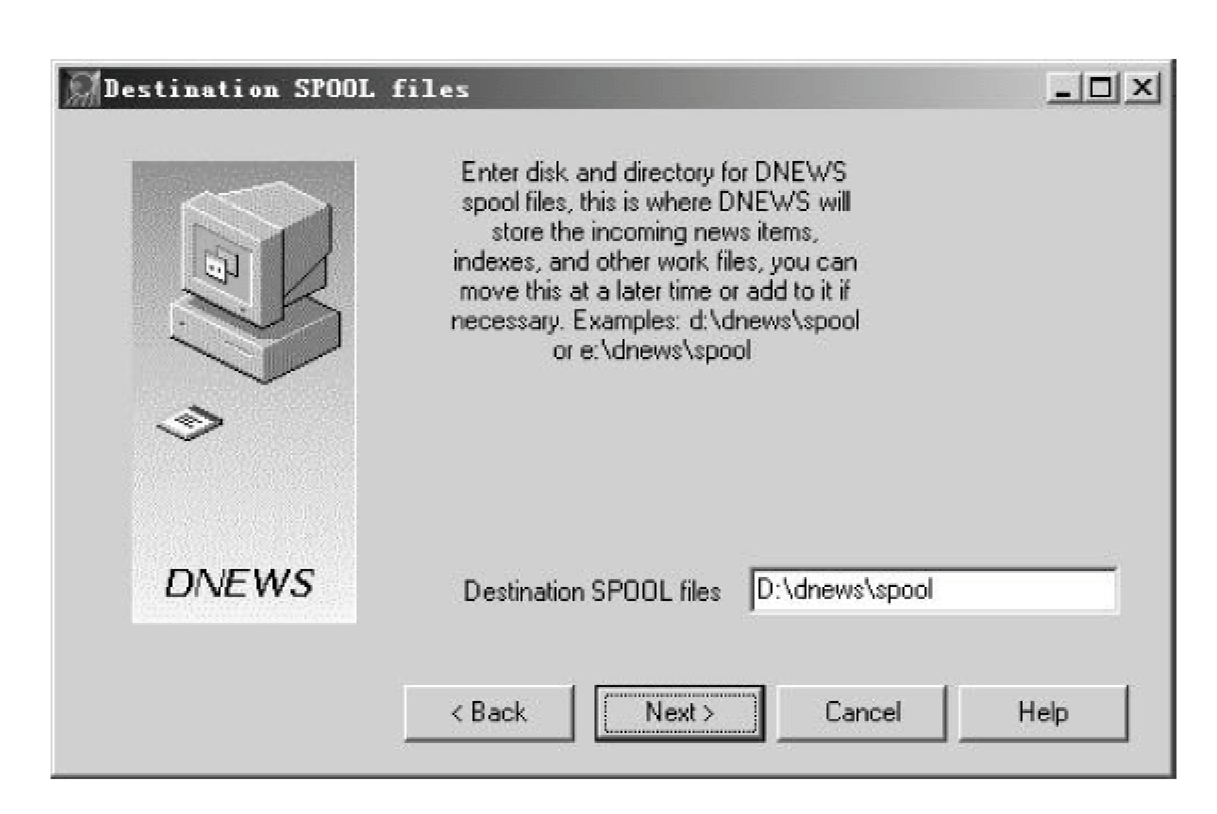


图 7-14　Destination SPOOL files 对话框

D:\dnews\spool,然后单击 Next 按钮。

(13) 此时出现 How many MB available 对话框,如图 7-15 所示,提示用户设定新闻组服务器安装分区最大使用空间。How many MB available 文本框中的默认值随安装设置的不同会发生相应的变化,如本次安装过程中出现的此默认值是 13840。可以改变该值,但要注意的是输入的数值不要大于此默认值。通常使用默认值即可,然后单击 Finish 按钮。

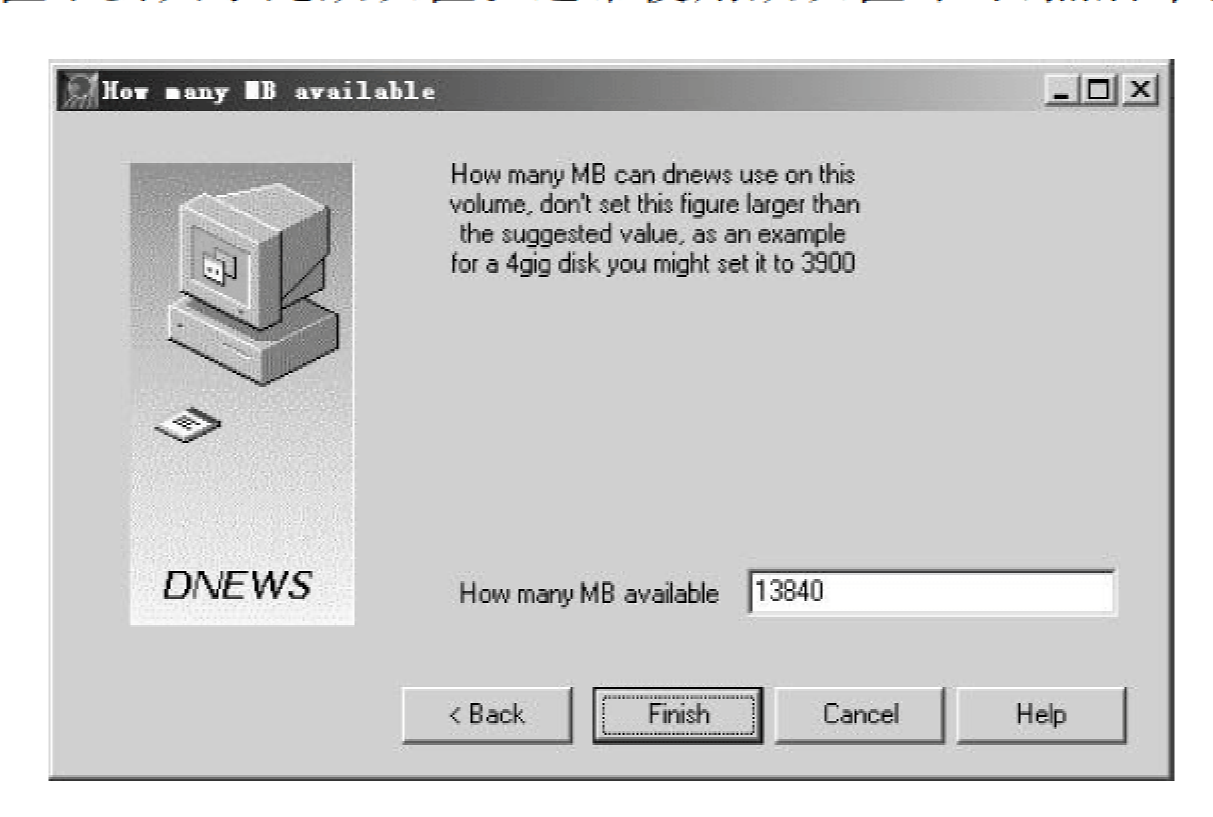


图 7-15　How many MB available 对话框

(14) 此时出现 Alert 对话框,如图 7-16 所示,提示用户安装成功完成。在 Alert 对话框中单击 Ok 按钮,完成 DNews 软件的安装。

(15) 安装完成后,系统会自动启动 DNews,同时在屏幕上弹出 DNews 5.7el Admin Tool 管理工具窗口,如图 7-17 所示。



图 7-16　Alert 对话框

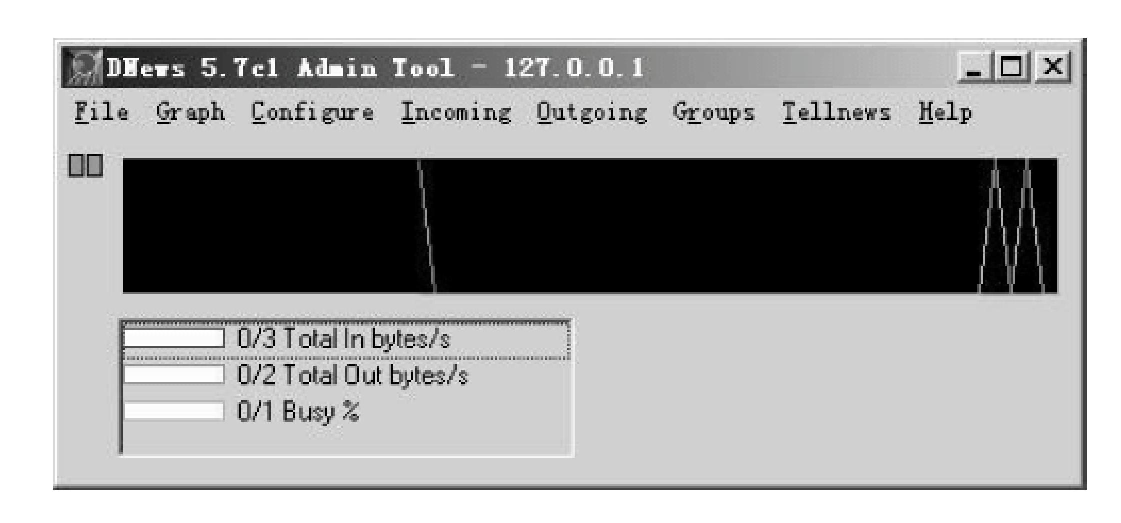


图 7-17　DNews 5.7el Admin Tool 管理工具窗口



7.3 DNews 服务器端的配置与管理

DNews 提供了三种方式对新闻组服务器进行配置和管理，分别是图形界面的 DNews 管理工具方式、字符界面的 DOS 命令行方式、基于 Web 界面的远程管理方式。

其中，字符界面的 DOS 命令行方式是在【命令提示符】窗口通过 Tellnews 命令来实现配置和管理功能，是早期版本的 DNews 服务器采用的主要形式，目前其功能可以通过图形界面的 DNews 管理工具的 Tellnews 菜单完全实现。因此这里不再赘述。

图形界面的 DNews 管理工具功能强大，可以实现所有的管理功能，并且界面直观，是主要的管理方式，也是本节重点介绍的管理方式。

而基于 Web 界面的远程管理方式实际上是通过 DNews 提供的基于 Web 的管理程序 DMGRCGI 来实现远程管理功能，它通过网络使用 7119 端口与服务器进行通信，可以在【命令提示符】窗口用 net stop dmgrsvc 停止其服务，也可以通过选择【控制面板】→【服务】启动/停止其服务。

前述任何一种管理方式实际上都是通过对 DNews 服务器的 6 个配置文件进行编辑修改来实现的。6 个配置文件（*.conf）的说明如表 7-3 所示。

表 7-3　DNews 的 6 个配置文件

文件名称	说　明
dnews. conf	DNews 服务器主配置文件，所在目录“\windows\system32”
newsfeeds. conf	定义新闻服务器的 FEED(供给)服务，所在目录为 DNews 安装目录
expire. conf	定义新闻条目的过期规则，所在目录为 DNews 安装目录
moderators. conf	定义仲裁新闻组的邮件地址，所在目录为 DNews 安装目录
access. conf	控制 NNTP 协议访问服务器的存取权限，所在目录为 DNews 安装目录
control. conf	定义自动创建和删除新闻组时的控制信息的处理，所在目录为 DNews 安装目录

提示：这 6 个配置文件都是文本文件，可以用任何文本编辑器打开修改。

7.3.1 通过 DNews 5.7e1 管理工具配置与管理服务器

如前所述，对 DNews 服务器端的配置与管理主要是通过 DNews 5.7e1 Admin Tool 管理工具程序来实现的。安装完成后，系统会在后台自动启动 DNews 服务，同时自动启动其管理工具程序。但是以后每次重新启动操作系统时，虽然 DNews 服务都会在后台自动启动，但其管理工具程序却不会自动启动。而且与其他软件有所不同，DNews 安装后其程序组不会出现在 Windows 2003 的程序菜单中。因此，为了方便对 DNews 服务器进行配置与管理，用户可以将“\windows\system32”目录下的 DNews 管理工具程序文件 dadmin.exe 复制到桌面上或者在桌面上建立快捷方式，以方便以后的配置与管理操作。

借助于 DNews 提供的管理工具，管理员可以快速建立新闻组，并严格控制新闻组权



限，达到安全信息访问的目的。通过存取控制，可以快速配置新闻转发及新闻下载，即可以从其他服务器上下载(suck)新闻，或将本地信件转发到外部新闻服务器上。这里仅以最常见的配置和管理操作进行说明。

1. 监控新闻组服务器运行情况

在图 7-17 所示的 DNews 5.7e1 Admin Tool 管理工具窗口，可以直观方便地监控新闻组服务器运行情况。菜单栏下方的黑色窗口和左下角的条格窗口是用来显示 DNews 服务器运行情况的，包括新闻组帖子的流入和流出情况以及新闻组服务器的繁忙情况。其中，红线表示帖子流入情况，绿线表示帖子流出情况，蓝线表示服务器繁忙情况。

2. DNews 新闻组服务器的启动和停止

DNews 所有操作都可以通过 DNews 5.7e1 Admin Tool 管理工具窗口完成，包括服务器的启动和停止等操作。在 DNews 5.7e1 Admin Tool 管理工具窗口的菜单栏中打开 File 菜单，如图 7-18 所示。

(1) 要启动新闻组服务器，选择 Start DNews 命令即可。

(2) 要停止新闻组服务器，选择 Stop DNews 命令即可。

(3) 要设置 DNews 新闻组服务器管理员口令，选择 Set Local Password 命令即可。

3. 建立本地新闻组

(1) 在 DNews 5.7e1 Admin Tool 管理工具窗口的菜单栏中打开 Groups 菜单，如图 7-19 所示。

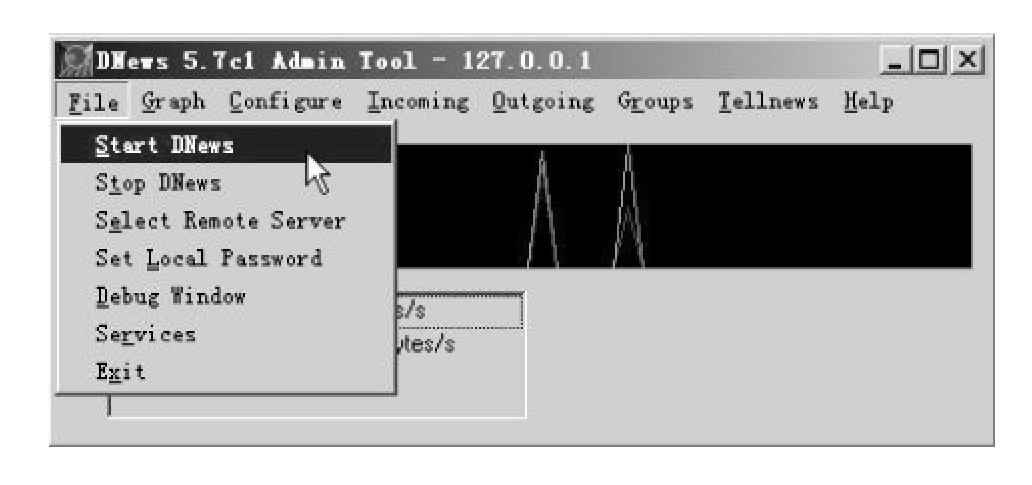


图 7-18　File 菜单

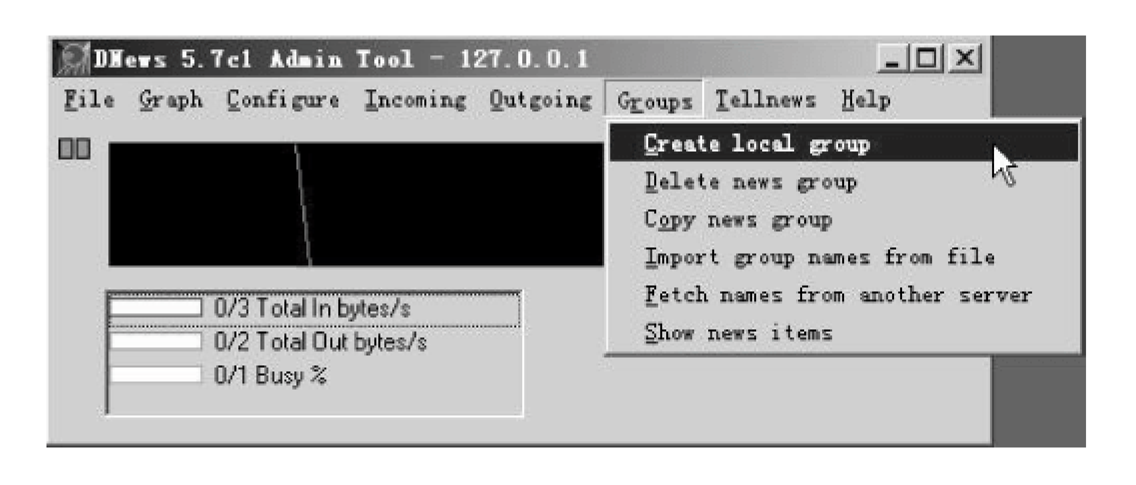


图 7-19　Groups 菜单

(2) 选择 Create local group 命令，会弹出 Create New Group 对话框，如图 7-20 所示。在 Enter name of new group 文本框中输入待添加的新闻组名称(这里输入 group.chapter7)，在 Description (optional)文本框中输入该新闻组的描述信息(这里输入“第七章测试新闻组”)，单击 Ok 按钮。

(3) 弹出 Tellnews Results 对话框，如图 7-21 所示。直接单击 Ok 按钮，完成新闻组 group.chapter7 的建立。

(4) 用同样方法再建立一个名为 group.test 的新闻组。

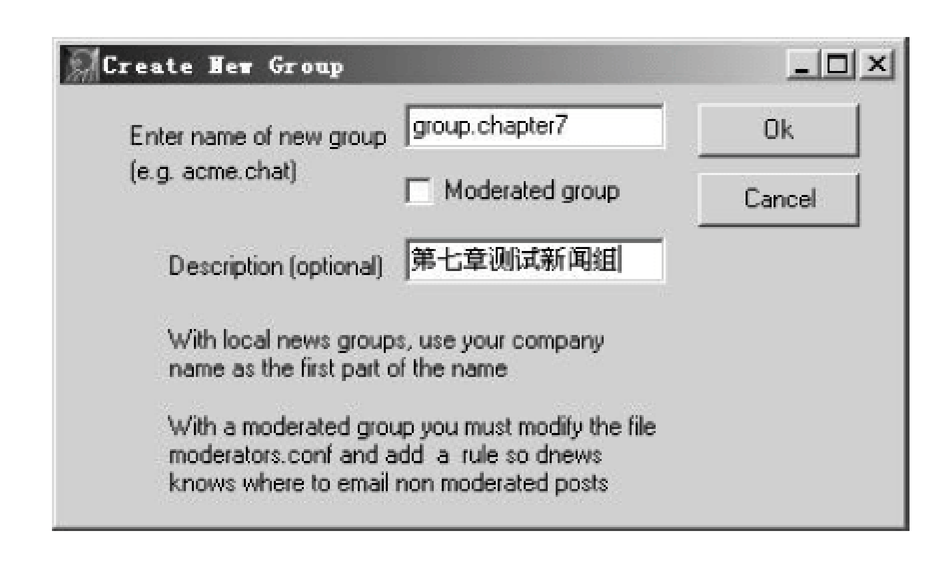


图 7-20　Create New Group 对话框



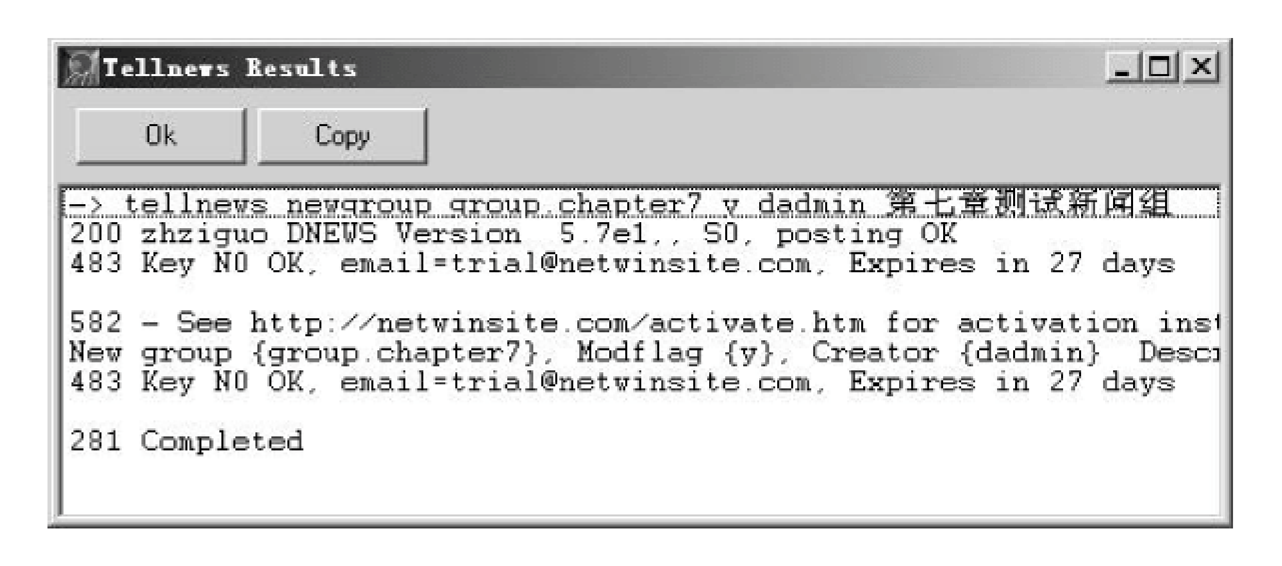


图 7-21　Tellnews Results 对话框

4. 复制新闻组

（1）在图 7-19 所示菜单中选择 Copy news group 命令，会弹出 Name of source group to copy 对话框，如图 7-22 所示。在 Name of source group to copy 文本框中输入要复制的源新闻组名称（这里输入 group. chapter7），单击 Ok 按钮。

（2）弹出 Name of destination group 对话框，如图 7-23 所示。在 Name of destination group 文本框中输入要复制的目标新闻组名称（这里输入 group. test），单击 Ok 按钮。

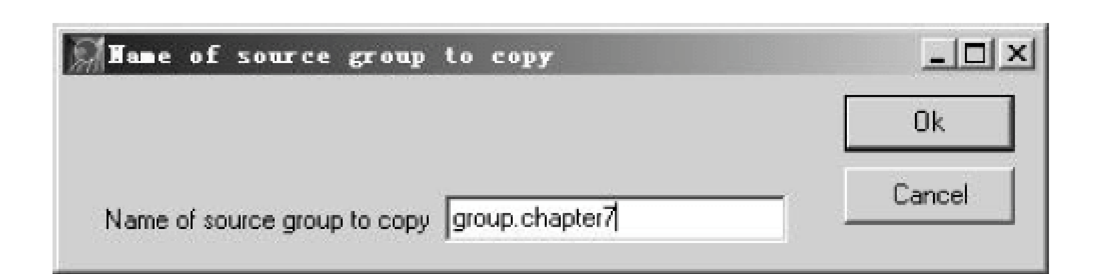


图 7-22　Name of source group to copy 对话框

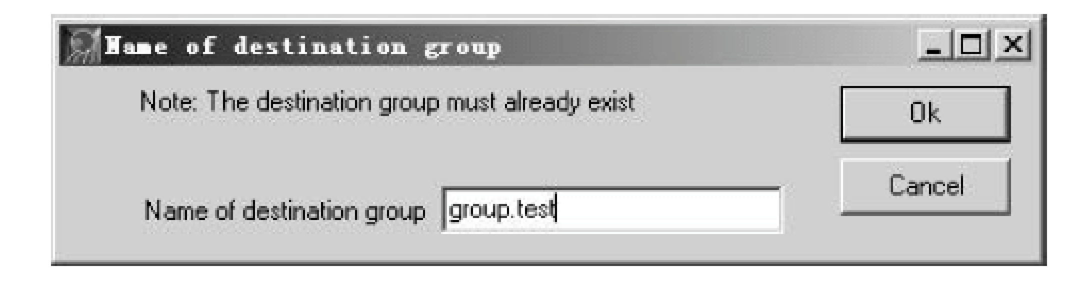


图 7-23　Name of destination group 对话框

（3）弹出 Tellnews Results 对话框，如图 7-24 所示。直接单击 Ok 按钮，完成新闻组的复制，现在新闻组 group. test 的内容与 group. chapter7 的完全一致。

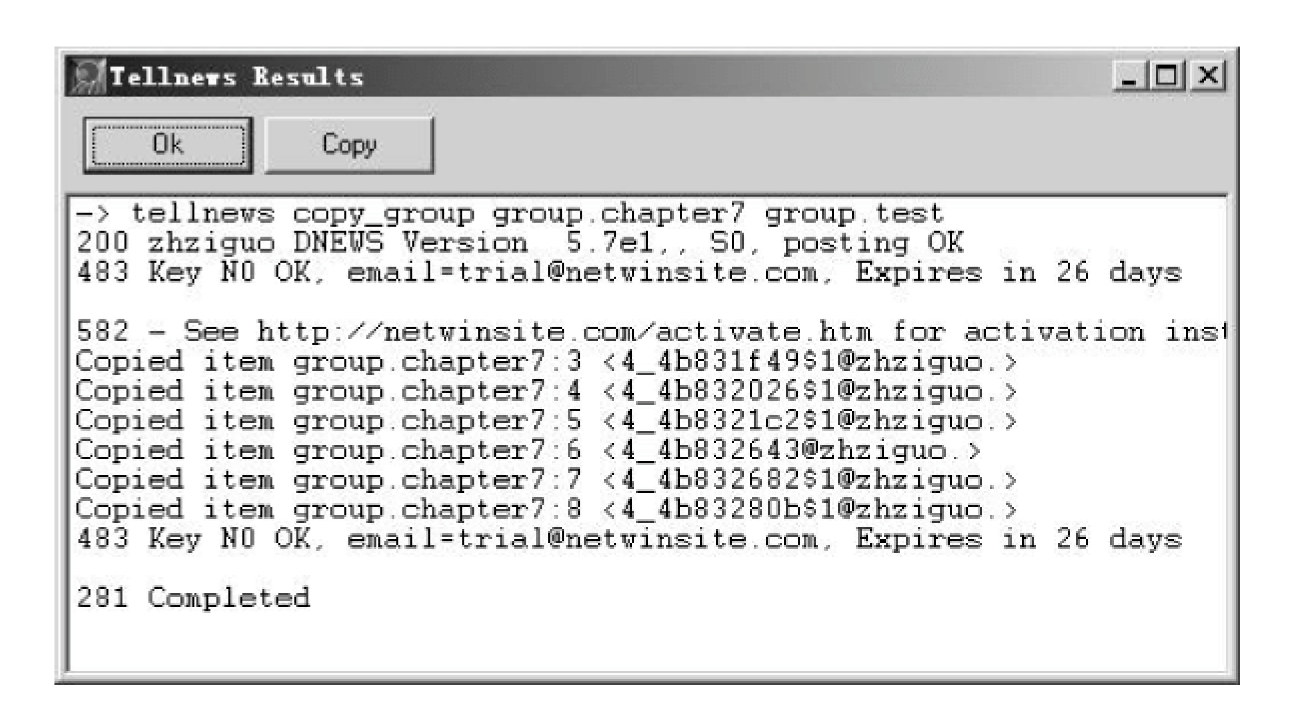


图 7-24　Tellnews Results 对话框

5. 删除新闻组

（1）在图 7-19 所示菜单中选择 Delete news group 命令，会弹出 Group to delete 对话框，如图 7-25 所示。在 Group to delete 文本框中输入要删除的新闻组名称（这里输入 group. test），单



图 7-25　Group to delete 对话框





击 Ok 按钮。

(2) 弹出 Tellnews Results 对话框,如图 7-26 所示。直接单击 Ok 按钮,完成新闻组 group.test 的删除。

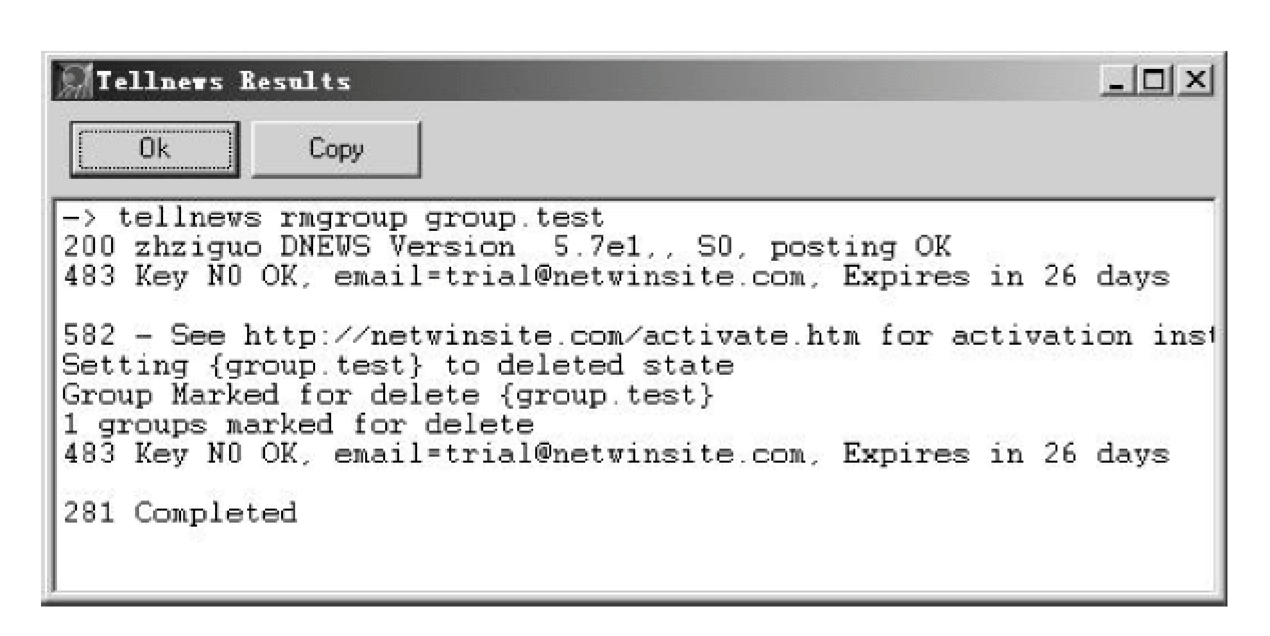


图 7-26 Tellnews Results 对话框

6. 新闻组服务器的卸载

当不再需要 DNews 或其出现严重故障需重新安装时,需要将其卸载。这时可以通过 DNews 5.7el Admin Tool 管理工具软件自身具备的卸载功能进行卸载。

在 DNews 5.7el Admin Tool 管理工具窗口的菜单栏中打开 Configure 菜单,选择 Uninstall DNEWS 命令即可完成卸载如图 7-27 所示。

7. 设置新闻组服务器的接收规则

为了避免 DNews 在接收新闻信息时受到垃圾信息的干扰,需要对 DNews 服务器接收新闻组的规则进行相应设置,从而无论是从本地服务器上,还是从其他新闻服务器上接收新闻信息,都可以控制对新闻信息进行接收或拒绝。这样既能降低不必要的网络流量,又可避免垃圾信息的传入。

具体的操作步骤如下:

(1) 在 DNews 5.7el Admin Tool 管理工具窗口的菜单栏中打开 Incoming 菜单,如图 7-28 所示。

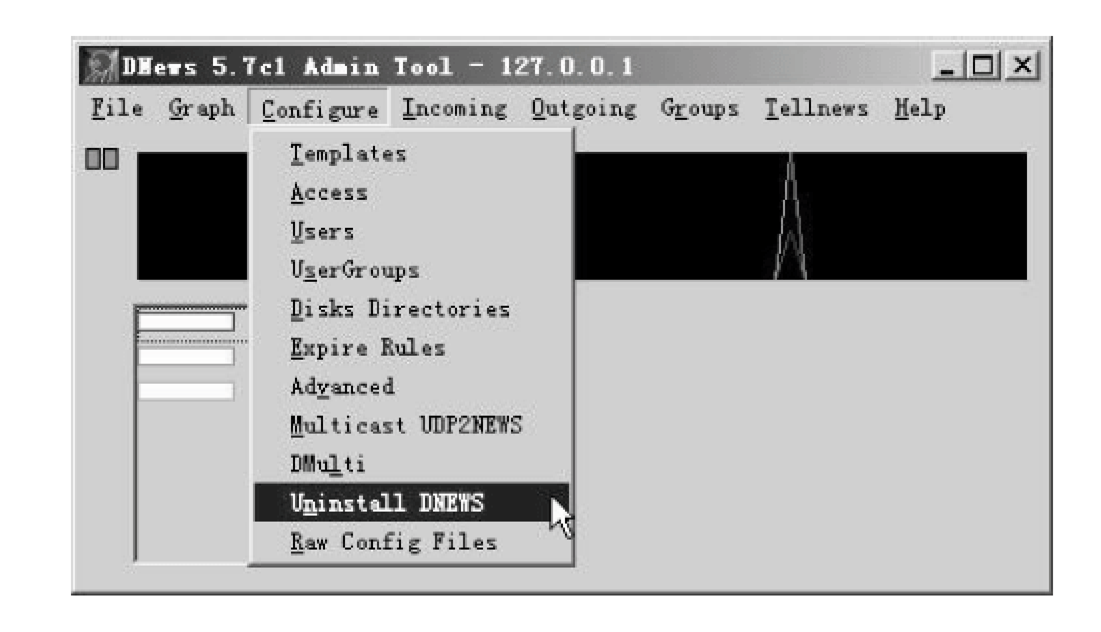


图 7-27 新闻组服务器的卸载

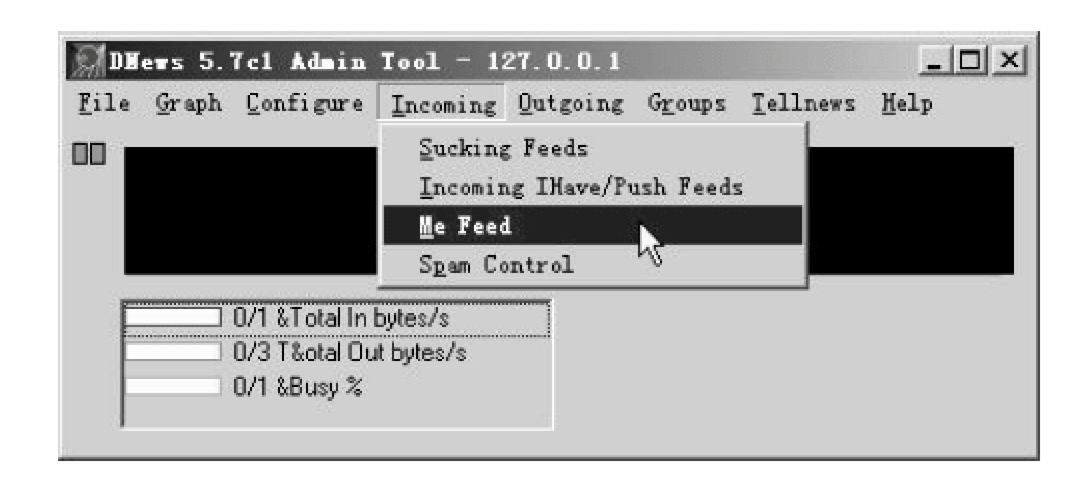


图 7-28 Incoming 菜单

(2) 选择 Me Feed 命令,会弹出 ffeed2 对话框,如图 7-29 所示。

在 Site to send feed to 文本框中输入发送新闻的目的服务器(这里使用默认值 me,代表本地新闻服务器)。



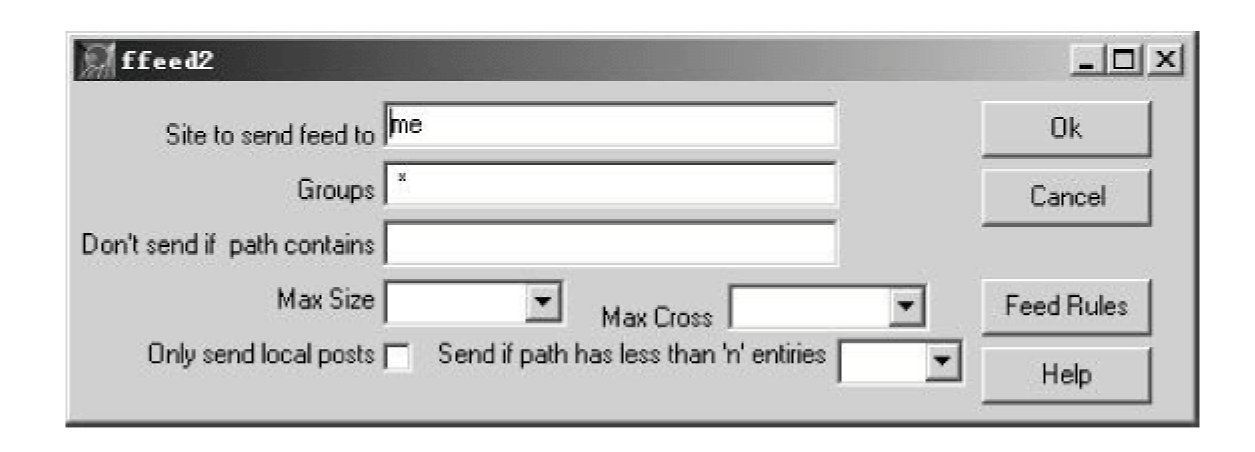


图 7-29　ffeed2 对话框

在 Groups 文本框中输入要接收的新闻组服务器名称。这里如果输入多个服务器，要使用英文半角的“，”隔开。还可以使用“＊”通配符，代表接收所有的新闻组。

在 Don't send if path contains 文本框中输入要过滤的文本内容。这样路径标题中包含这些内容的新闻将不会被接收。

在 Max Size 列表框中设置新闻条目的最大文件尺寸。

在 Max Cross 列表框中设置新闻条目跨越新闻服务器的最大节点数量。

（3）单击 Feed Rules 按钮可以进一步定义接收规则，此时会弹出 Rules to apply to each message 对话框，如图 7-30 所示。已经定义的规则会在左侧列表框中列出。如果要定义新的规则，单击右侧的 Add Rule 按钮。

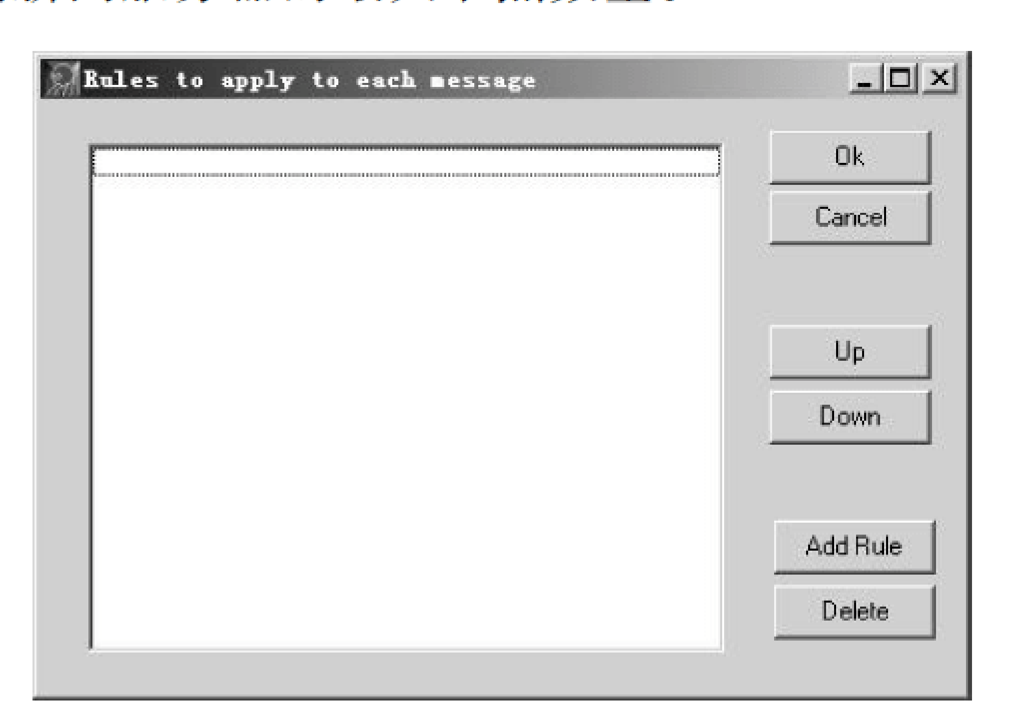


图 7-30　Rules to apply to each message 对话框

（4）此时会弹出 Define a rule for accepting or rejecting a message 对话框，如图 7-31 所示。其左侧列表框包含两个选项，accept 表示接受，reject 表示拒绝。中间列表框是对新闻条目限制的内容，比如用 subject 对新闻主题进行限制，用 body 对新闻正文进行限制，等等。右侧文本框则用来输入匹配条件，即具体的限制内容。最后单击 Ok 按钮，保存新设定的规则。设置完成，此时新的规则将会加入到图 7-30 所示对话框左侧的规则列表中。

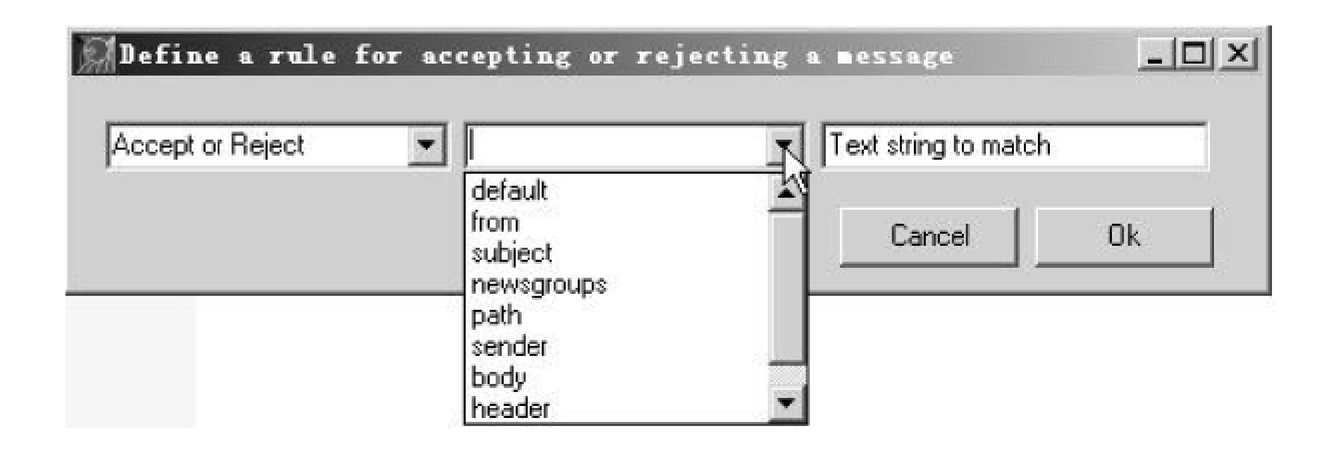


图 7-31　Define a rule for accepting or rejecting a message 对话框

8. 设置新闻组服务器的抓取（转信）规则

DNews 服务器可以从其他新闻服务器上抓取新闻条目，其抓取规则设置的具体操作步骤如下：

（1）在图 7-28 所示菜单中选择 Sucking Feeds 命令，会弹出 Configure Sucking Feeds



对话框,如图 7-32 所示。此时已经定义的规则会在左侧列表框中列出,可以双击进行编辑。如果要定义新的规则,则单击右侧的 Add Suck 按钮。

（2）此时会弹出 Modify Sucking Feed 对话框,如图 7-33 所示。

在 Groups to suck 文本框中输入要抓取新闻条目的源新闻组服务器,在 Update Times 文本框中选择抓取时间间隔,在 Send back to same host 选项区域中选择相应的复选框,在 Username、Password 文本框中输入新闻组服务器登录时的用户名和密码。

输入完毕之后,单击 Apply 按钮完成设置。

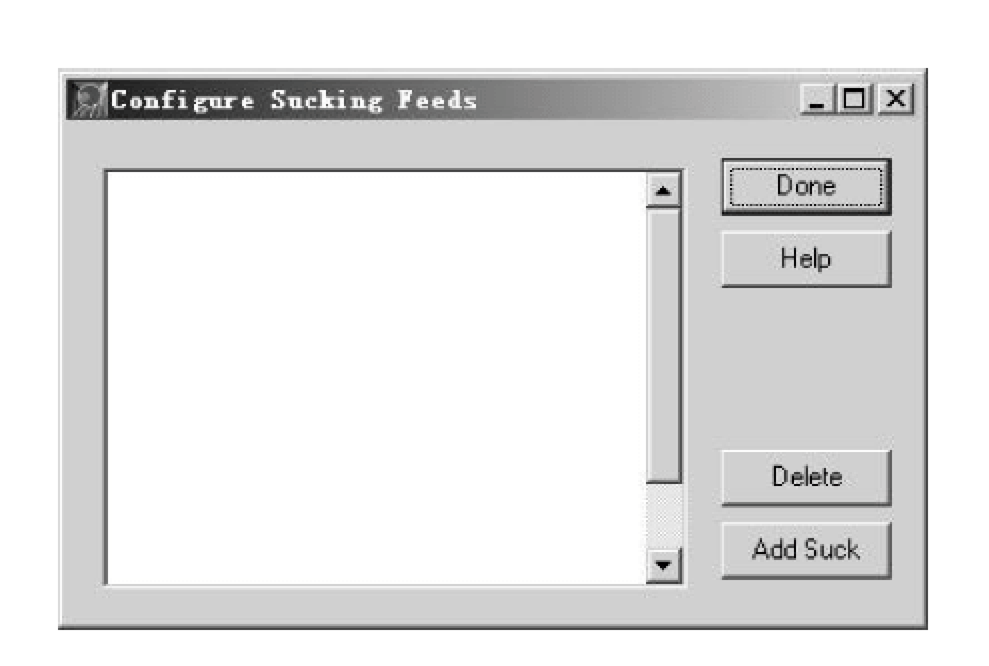


图 7-32　Configure Sucking Feeds 对话框

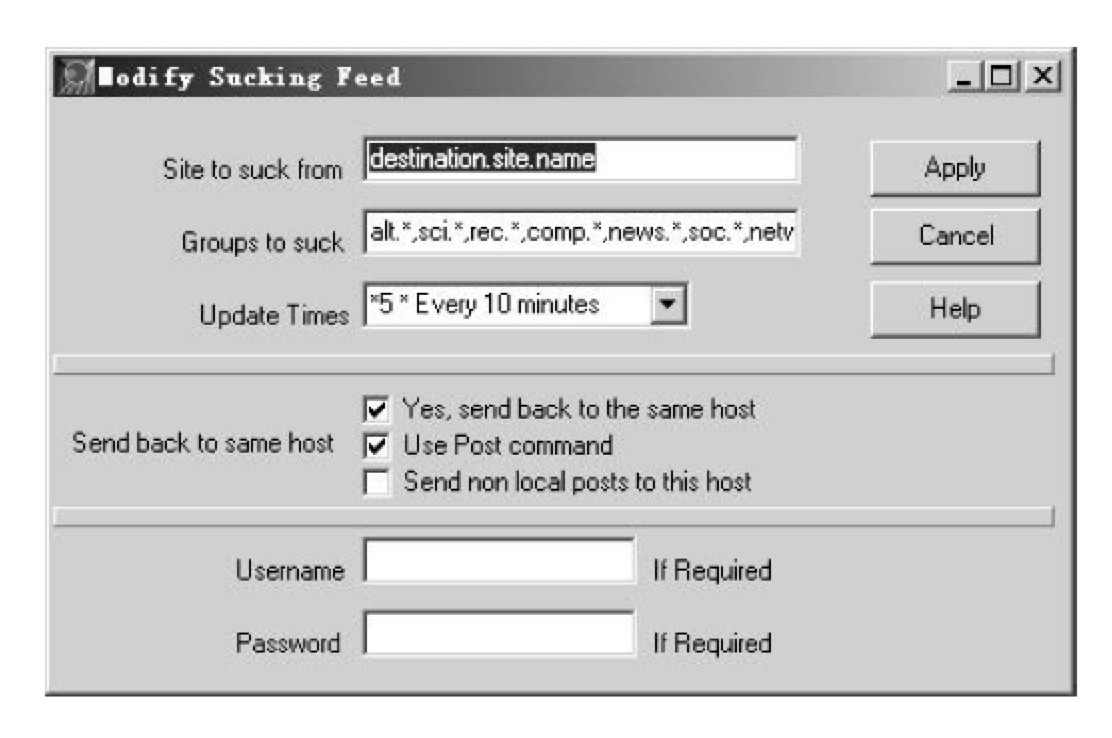


图 7-33　Modify Sucking Feed 对话框

9. 设置新闻组服务器的发送规则

DNews 服务器除了接收其他新闻组服务器的新闻之外,还可以将自己的新闻条目发送给其他新闻服务器,其发送规则也可以进行设置。

具体的操作步骤如下:

（1）在 DNews 5.7el Admin Tool 管理工具窗口的菜单栏中打开 Outgoing 菜单,如图 7-34 所示。

（2）选择 News Feeds 命令,会弹出 Outgoing News Feeds 对话框,如图 7-35 所示。

此时已经添加的目的新闻服务器会在左侧列表框中列出,可以双击进行编辑。如果要添加新的新闻服务器,则单击右侧的 Add 按钮。

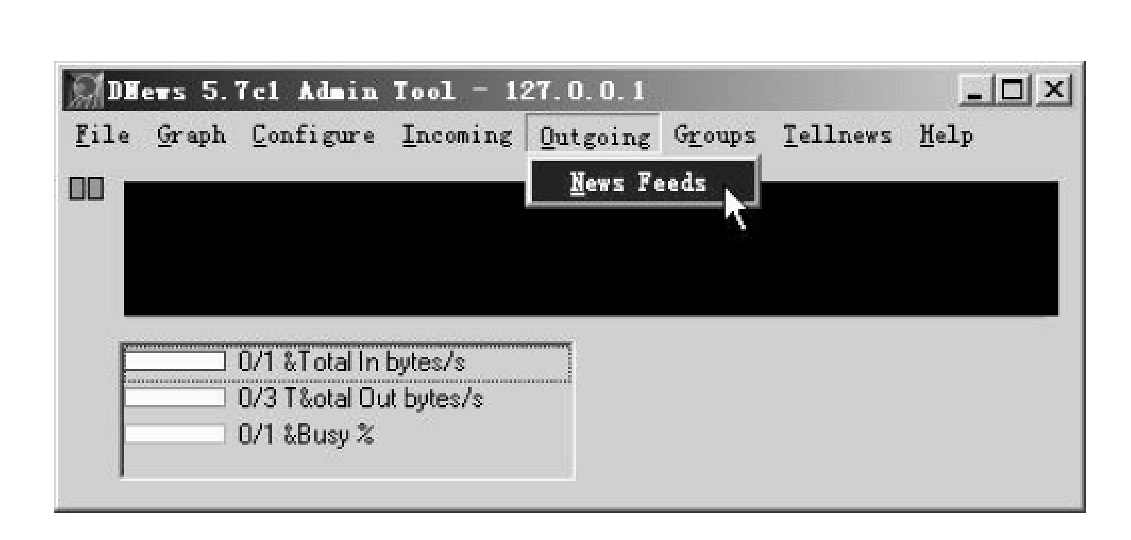


图 7-34　Outgoing 菜单

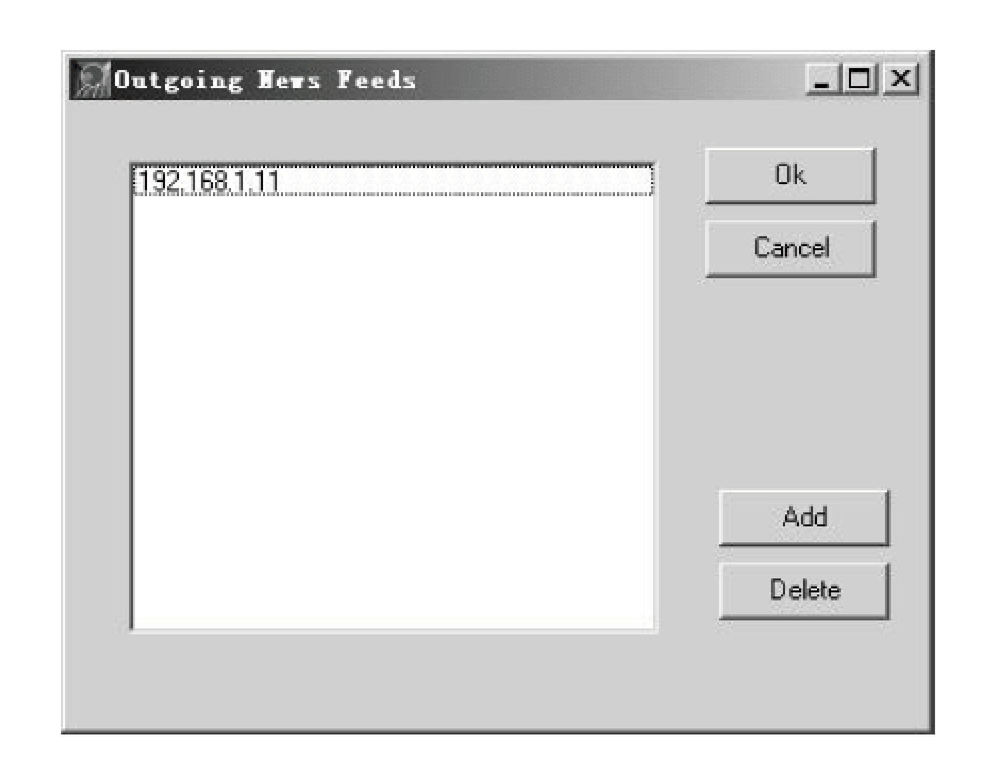


图 7-35　Outgoing News Feeds 对话框



(3) 此时会弹出 ffeed2 对话框，如图 7-36 所示。

在 Site to send feed to 文本框中输入新闻条目发送的目的服务器，在 Type of news feed 选项区域中选择新闻条目的发送类型，其余选项与图 7-29 中所示选项相同，在此不再赘述。

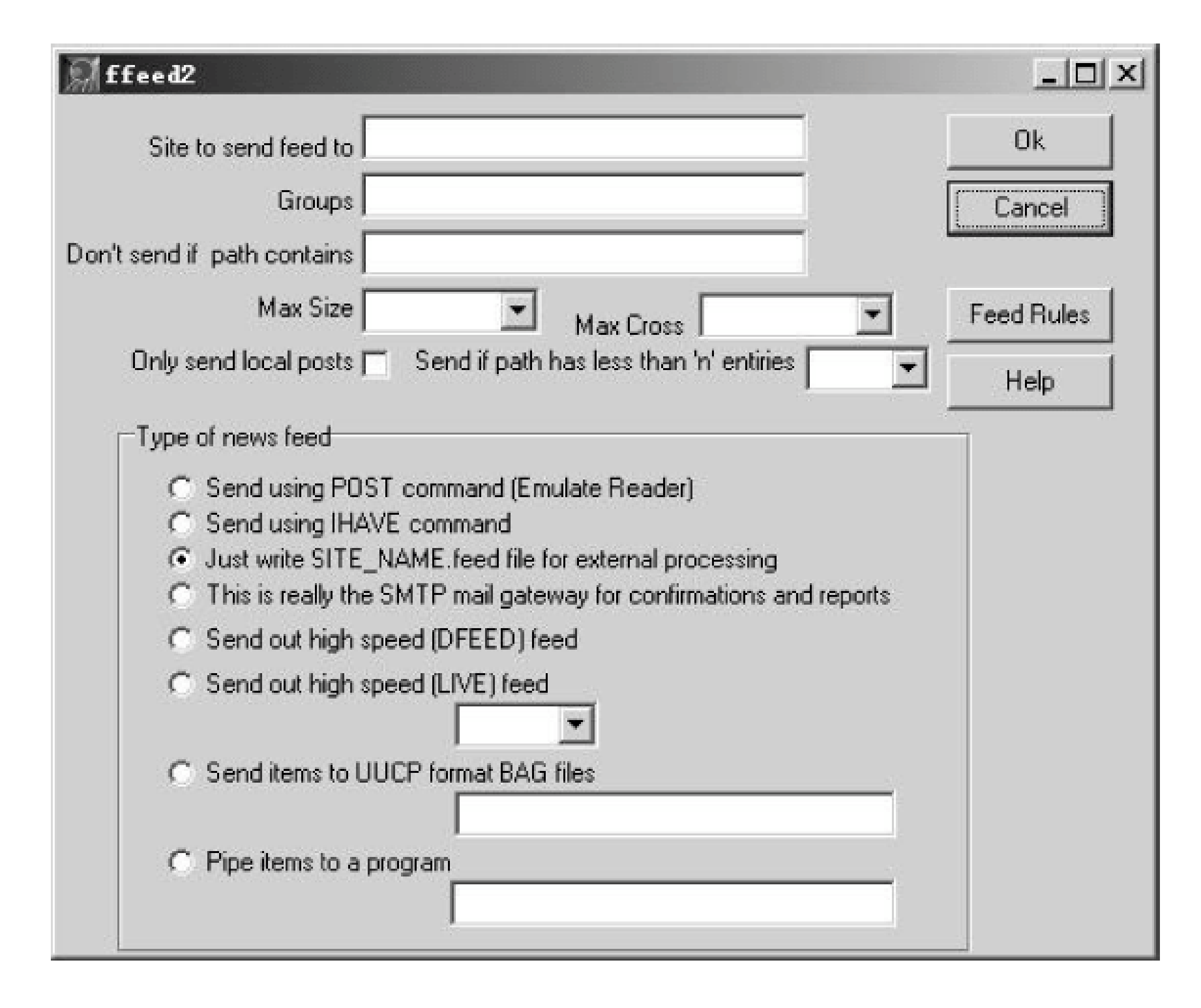


图 7-36　ffeed2 对话框

10. 管理新闻组中的帖子

在完成新闻组服务器软件的安装设置并组建了一系列的新闻组之后，还需要对新闻组进行相应的管理。由于所有的参与者都是以发帖子形式进行相关讨论的，因此，在对新闻组进行管理时，对帖子的管理是不容忽视的。

具体的操作步骤如下：

(1) 在图 7-19 所示菜单中选择 Show news items 命令，会弹出 Display news group, click on item to view 对话框，如图 7-37 所示。

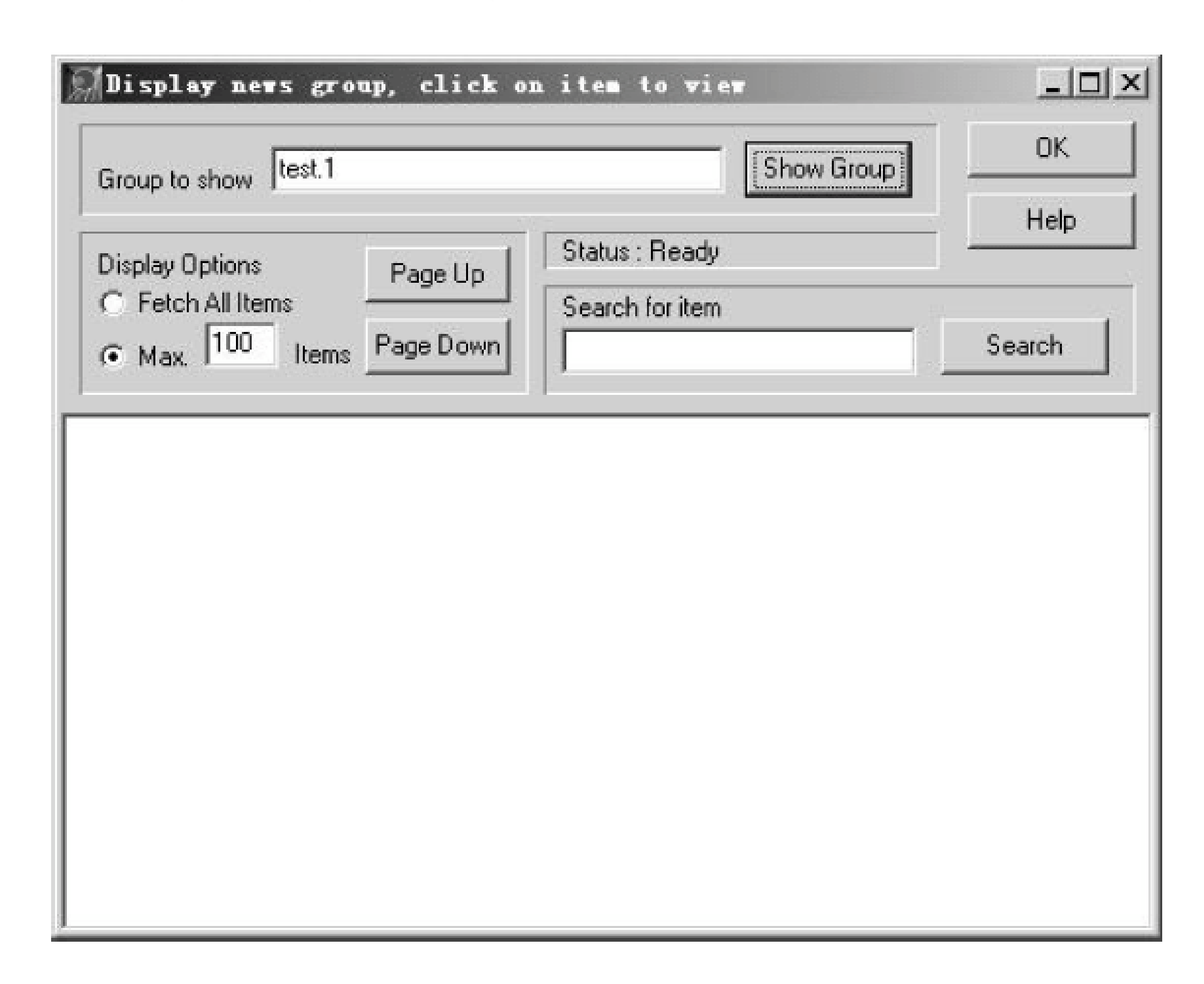


图 7-37　Display news group, click on item to view 对话框



(2) 在 Group to show 文本框中输入讨论组的名称，单击 Show Group 按钮，即可将讨论组的所有帖子显示到新闻组窗口下的文本框中。

(3) 选择 Fetch All Items 单选按钮即可将所有的帖子显示出来，选择 Max 100 Items 单选按钮则只显示最新帖子，单击 Page Up 和 Page Down 按钮可进行翻页操作。

(4) 在 Search for item 文本框中输入要找的帖子名称，单击 Search 按钮，即可快速找到自己所需要的帖子。

(5) 最后单击 Ok 按钮，即可完成对帖子的相应管理操作。

11. 设置用户登录时必须输入口令

由于参加新闻组进行讨论的人非常多，要想做到井然有序，就必须对用户进行相应的管理，对不同用户赋予不同的权限，并且要求用户登录时必须输入口令。

具体的操作步骤如下：

在图 7-27 所示菜单中选择 Access 命令，会弹出 Domains with access to read or post news 对话框，如图 7-38 所示。选择 Require users to always give passwords 复选框并单击 Done 按钮，即可设置成功。



图 7-38　Domains with access to read or post news 对话框

7.3.2　使用浏览器远程管理 DNews 新闻组服务器

DNews 新闻组服务器可以使用浏览器进行远程管理。要使用 Web 方式管理 DNews 新闻组服务器，首先需要在 DNews 5.7e1 Admin Tool 管理工具窗口添加具有远程管理权限的用户，然后再用该用户远程登录服务器，进行相应的设置和管理。

具体的操作步骤如下：

(1) 在图 7-27 所示菜单中选择 Users 命令，会弹出 Find/Add User 对话框，如图 7-39 所示。

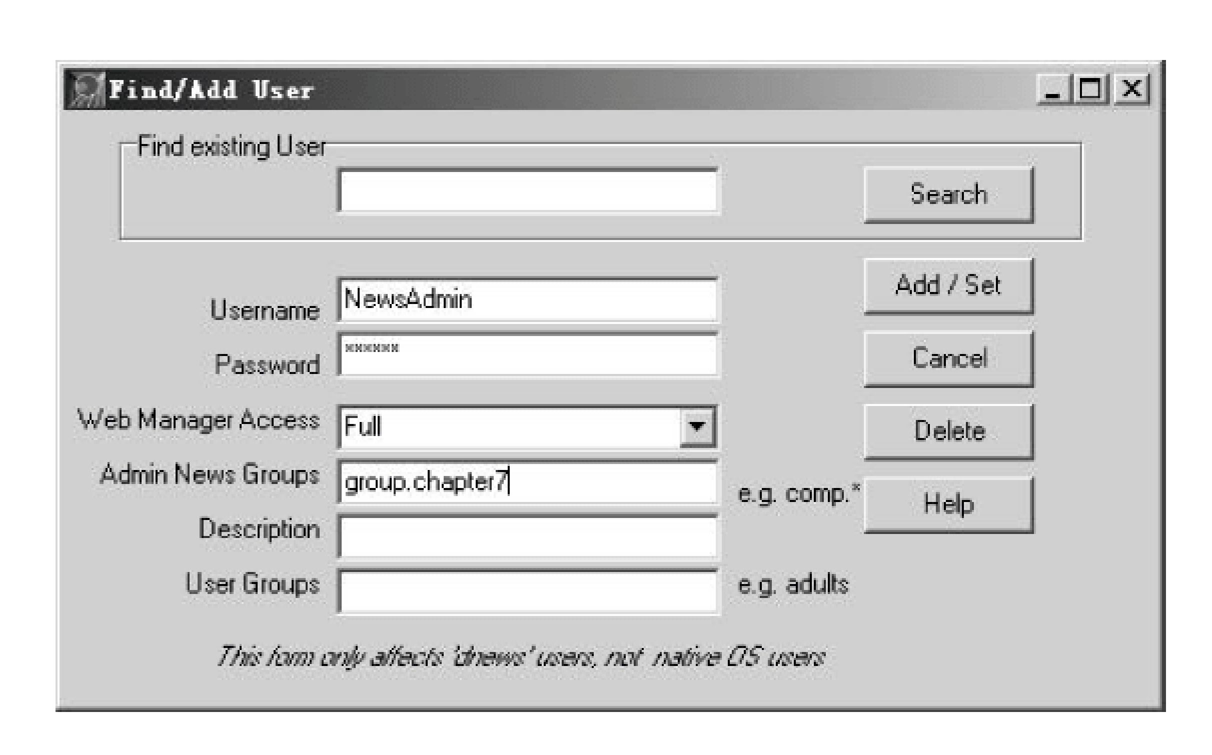


图 7-39　Find/Add User 对话框



在 Username 文本框中输入要创建的 DNews 用户名(注意不是计算机操作系统的用户名,这里输入 NewsAdmin);在 Password 文本框中输入该用户的访问口令(这里输入123456);在 Web Manager Access 文本框中选择该用户的管理员权限,共有 None、Tellnews、Users、Config、Full 五种权限,其中 Full 权限最高(这里选择 Full)。在 Admin News Groups 文本框中输入新闻组名称(这里输入 group. chapter7),其他选项空缺。填写完成后单击右侧的 Add/Set 按钮,用户账号创建完成。

(2) 打开 IE 浏览器,在地址栏中输入 http://news_server_ip_address:7119(这里为 http://192.168.1.11:7119)按 Enter 键,将显示【连接到 192.168.1.11】登录窗口。在这里输入刚才创建的管理员账户 NewsAdmin 及其密码 123456,如图 7-40 所示。单击【确定】按钮。



图 7-40　远程管理登录窗口

(3) 此时进入远程管理界面,系统首先显示服务器状态信息,如图 7-41 所示。可以看到,页面顶端是一行功能选项按钮,每选择一种功能选项,就可以在页面上进行相应设置。通过这个界面可以完成对 DNews 新闻组服务器的所有管理,下面以远程创建 DNews 账户 test2 的操作为例进行具体说明。

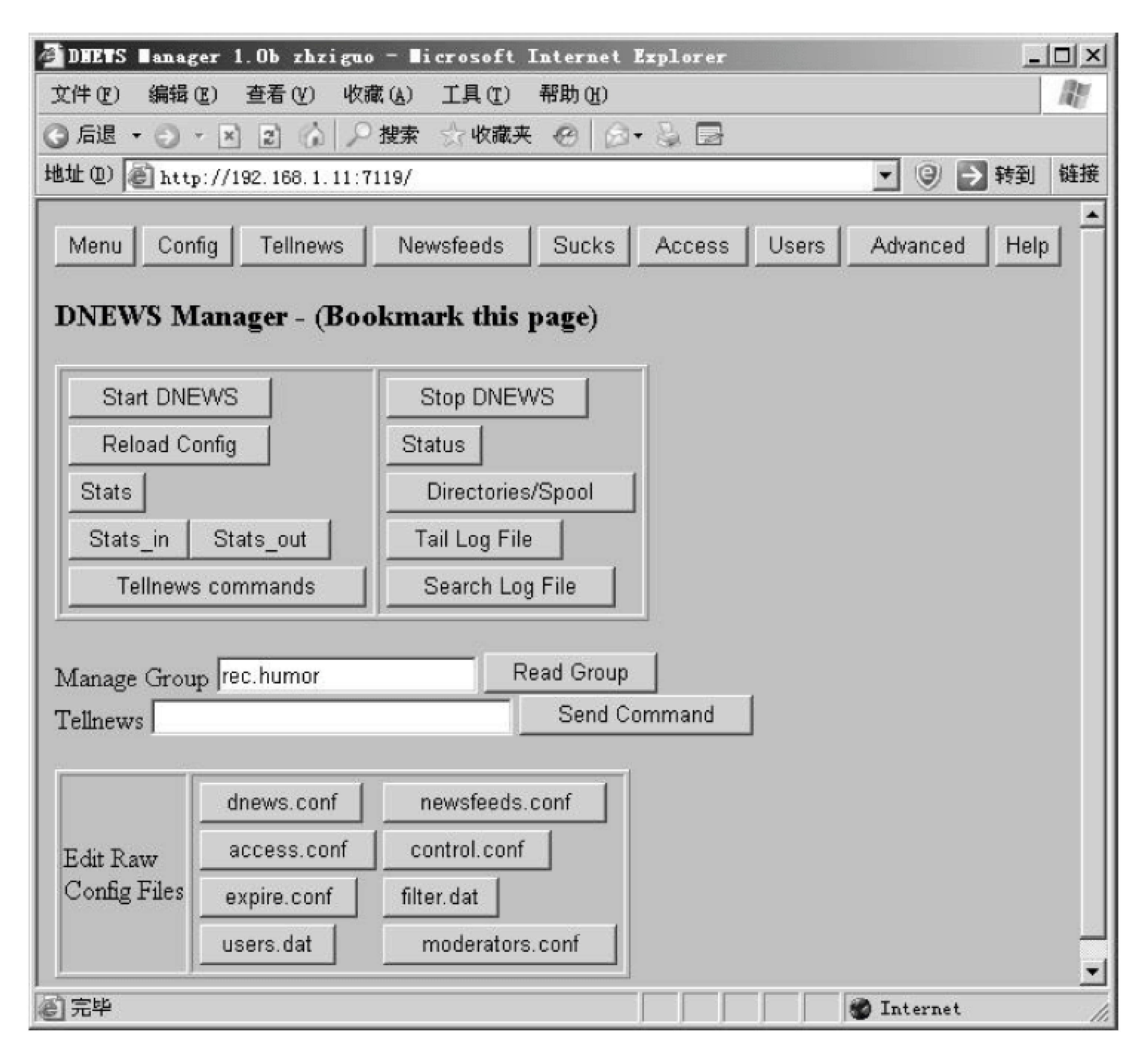


图 7-41　远程管理界面—DNews 管理

(4) 在页面顶端单击 Users 功能选项按钮,此时界面如图 7-42 所示。

在 User Name 文本框中输入要创建的 DNews 用户名(这里输入 test2),在 Password 文本框中输入该用户的访问口令(这里输入 test2),在 Manager Access 文本框中选择该用



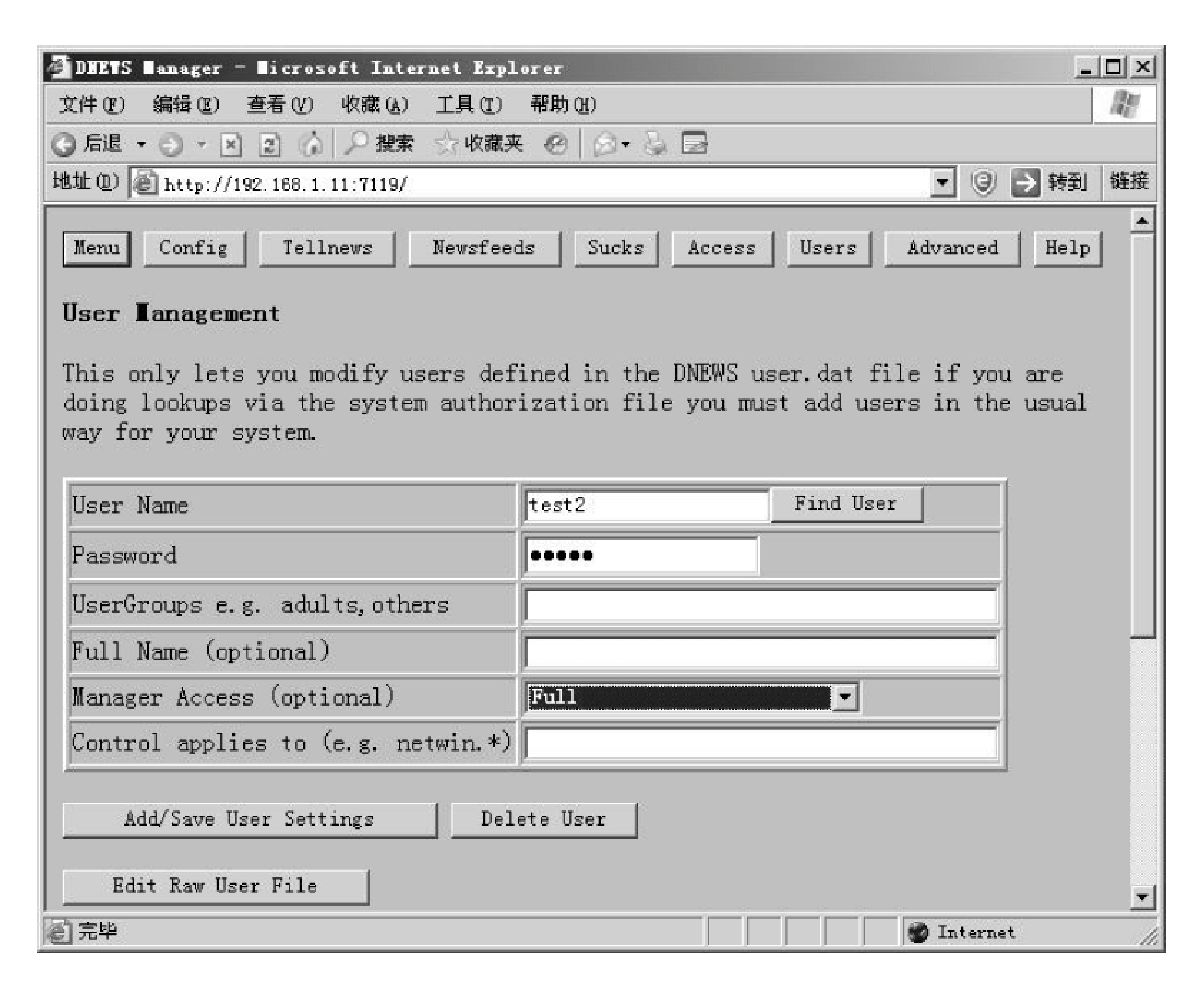


图 7-42 远程管理界面—用户管理

户的权限(这里选择 Full),其他选项空缺。填写完成后单击 Add/Save User Settings 按钮。

(5) 此时用户账号创建完成,界面如图 7-43 所示。



图 7-43 远程管理界面—创建新用户

7.4 客户端访问新闻服务器

在 DNews 服务器安装设置完毕后,就可以使用客户端进行访问了。

7.4.1 在客户端建立新闻账户

Outlook Express 是 Windows Server 2003 内置的邮件客户端,也是一款常用的新闻组客户端。这里就以 Outlook Express 为例进行说明。



(1) 在 Outlook Express 中选择【工具】→【账户】命令，如图 7-44 所示。



图 7-44　Outlook Express 的【工具】菜单

(2) 此时弹出【Internet 账户】对话框，如图 7-45 所示。单击【添加】按钮，选择其级联菜单中的【新闻】命令。



图 7-45　【Internet 账户】对话框

(3) 此时弹出【Internet 连接向导】对话框，如图 7-46 所示。在【显示名】文本框中填写 NewsGroupTest，单击【下一步】按钮。

(4) 此时的【Internet 连接向导】对话框如图 7-47 所示。在【电子邮件地址】文本框中填写该用户的电子邮件地址 test@test.com，单击【下一步】按钮。

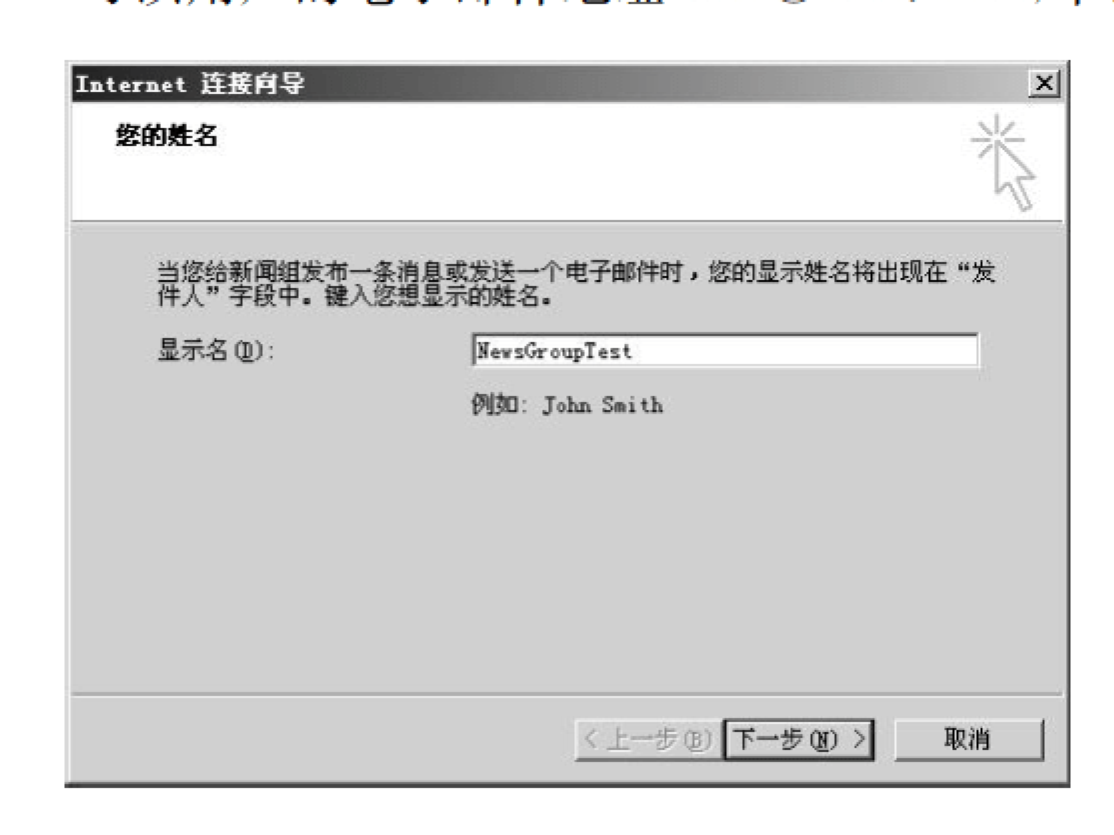


图 7-46　【Internet 连接向导】对话框——填写显示名



图 7-47　【Internet 连接向导】对话框——填写电子邮件地址





(5) 此时的【Internet 连接向导】对话框如图 7-48 所示。在【新闻(NNTP)服务器】文本框中输入上面建立的新闻服务器的 IP 地址 192.168.1.11,单击【下一步】按钮。

(6) 此时的【Internet 连接向导】对话框如图 7-49 所示。至此,新闻账户 NewsGroupTest 已经建立,单击【完成】按钮。

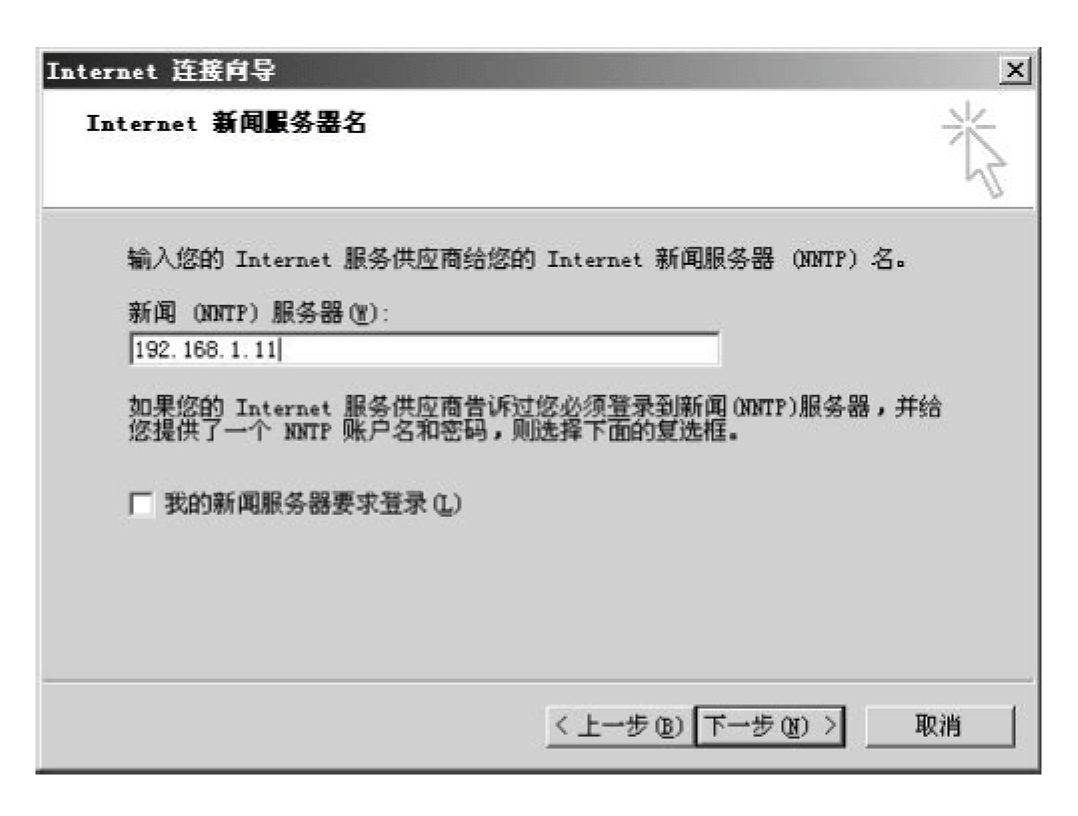


图 7-48 【Internet 连接向导】对话框—填写新闻服务器名



图 7-49 【Internet 连接向导】对话框—完成账户信息录入

(7) 此时系统会自动切换到【Internet 账户】对话框,从中可看到新增加的账户信息,如图 7-50 所示。单击【关闭】按钮。

(8) 此时弹出 Outlook Express 提示对话框,如图 7-51 所示。单击【是】按钮。

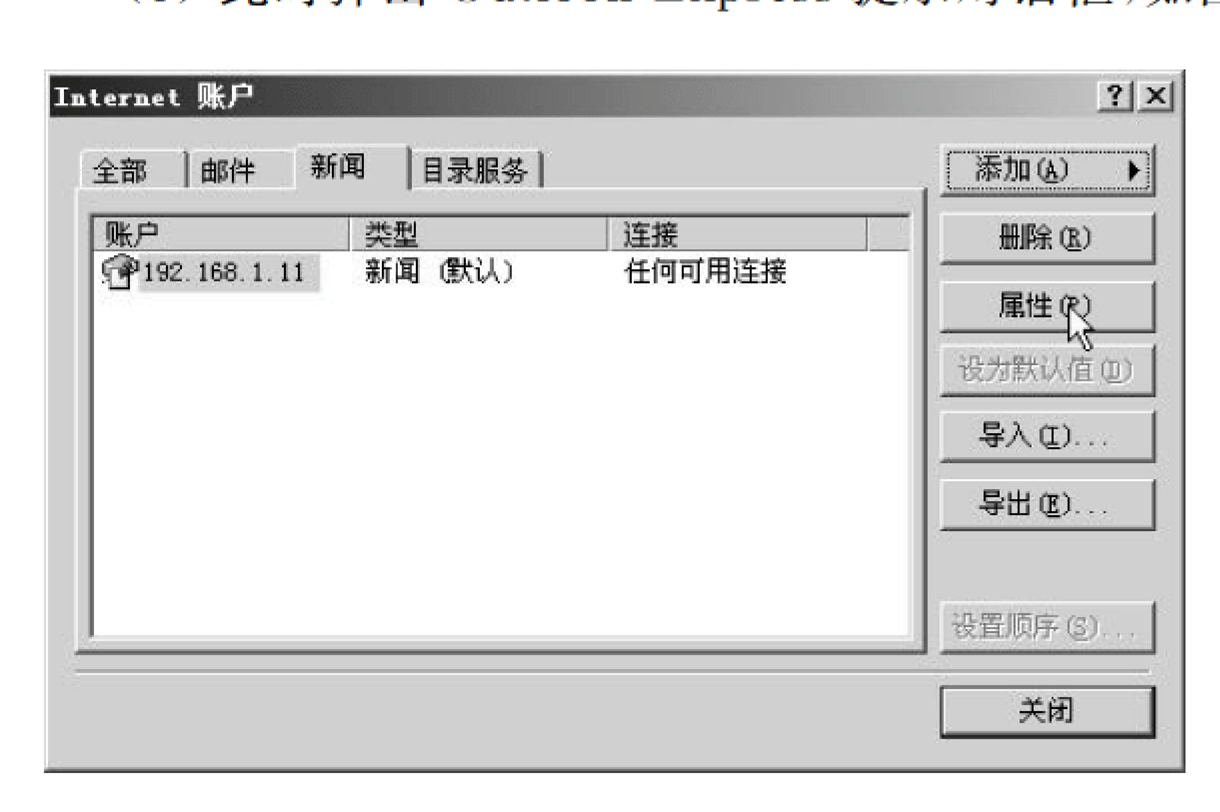


图 7-50 【Internet 账户】对话框

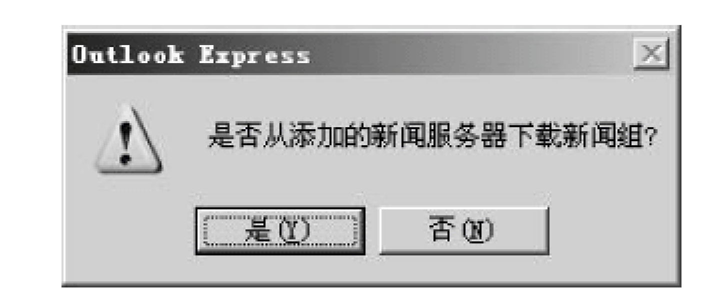


图 7-51 Outlook Express 提示对话框

(9) Outlook Express 自动从刚添加的新闻服务器上下载新闻组,并弹出【新闻组预订】对话框,如图 7-52 所示。可以看到,系统自动连接到了刚设定的新闻组服务器 192.168.1.11,并下载得到其中所有新闻组的列表。之前在该服务器上建立了新闻组 group.chapter(另一个新闻组 group.test 已经删除),在该对话框的新闻组列表中可以看到这个新闻组的名称。在列表中选中这个新闻组,然后单击右上角的【订阅】按钮。

(10) 此时在该新闻组前会马上出现一个表示“已预订”的小图标,如图 7-53 所示。单击【确定】按钮完成预订。





图 7-52 【新闻组预订】对话框—订阅



图 7-53 【新闻组预订】对话框—完成预订

7.4.2 为新闻组设定规则

为了更加有效率地使用新闻组，需要对 Outlook Express 进行一些其他的基本设置并设立新闻组规则。具体操作步骤如下：

(1) 在 Outlook Express 中选择【工具】→【选项】命令，在弹出的【选项】对话框中选择【阅读】选项卡，如图 7-54 所示。

在【阅读邮件】选项区域的【突出显示被跟踪的邮件】列表框中选择“红色”或其他醒目的颜色，这个选项将在下面设置新闻组规则中起作用。在【新闻】选项区域的【每次获取[300]个邮件标头】上下控件中，可自行改变下载标题的数量。这里使用默认值 300。

(2) 在 Outlook Express 中选择【工具】→【选项】命令，在弹出的【选项】对话框中选择【发送】选项卡，如图 7-55 所示。

在【新闻发送格式】选项区域中选中【纯文本】单选按钮，单击右方的【纯文本设置】按钮。



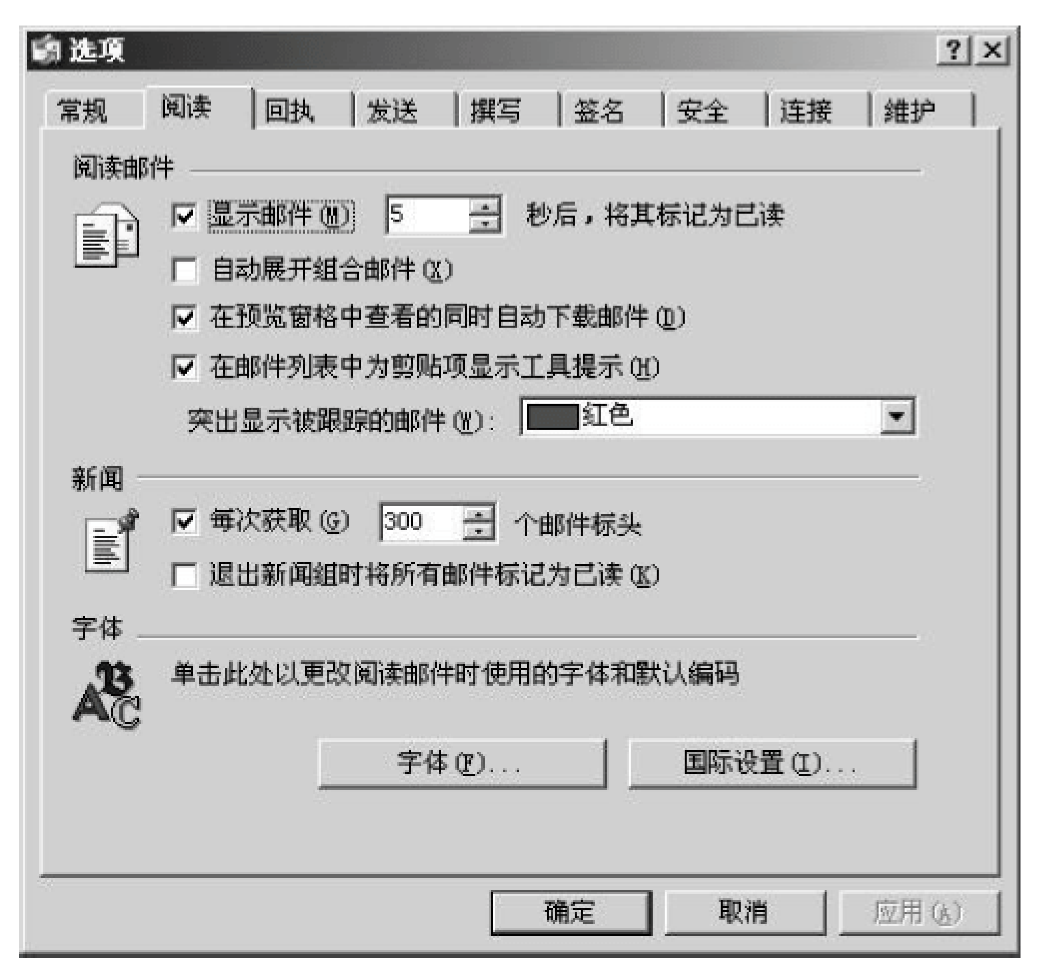


图 7-54　【选项】对话框—【阅读】选项卡

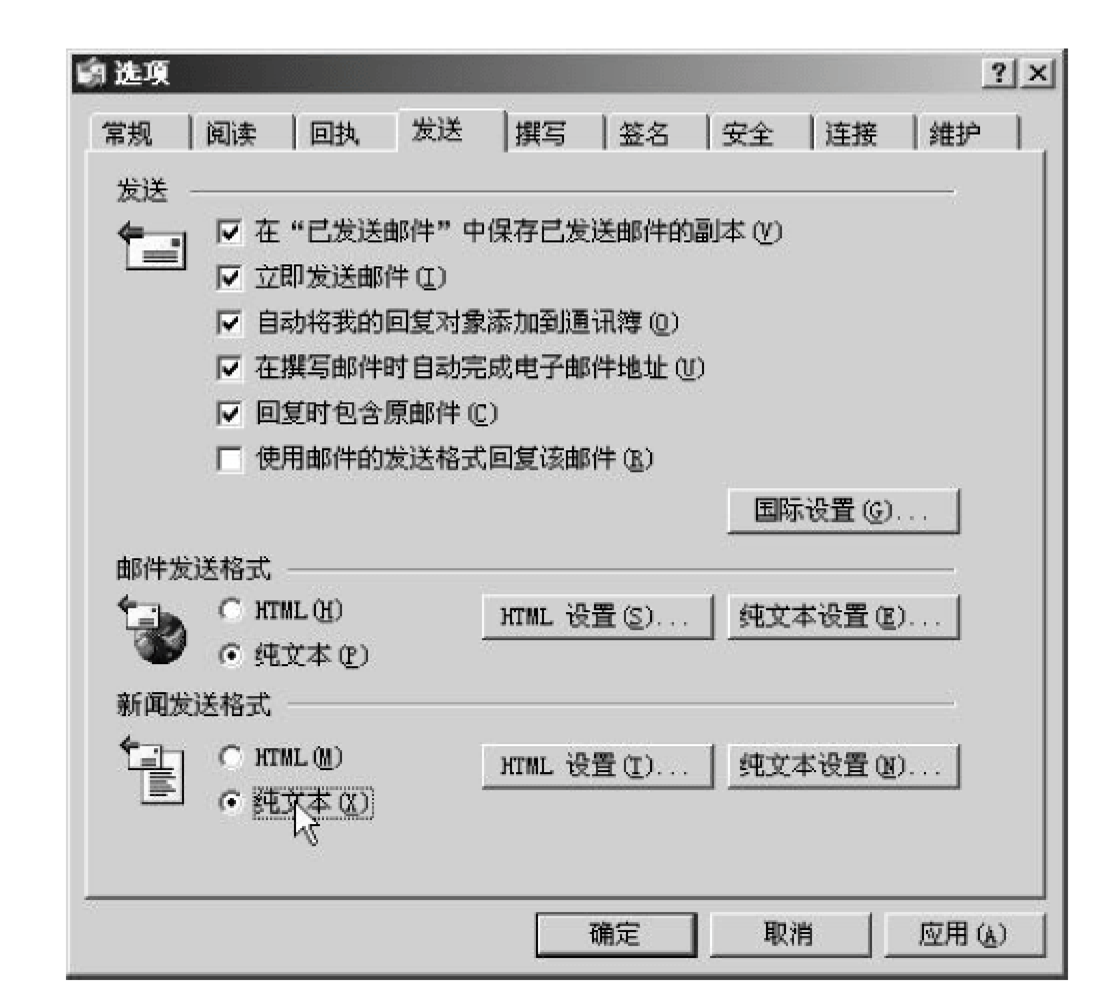
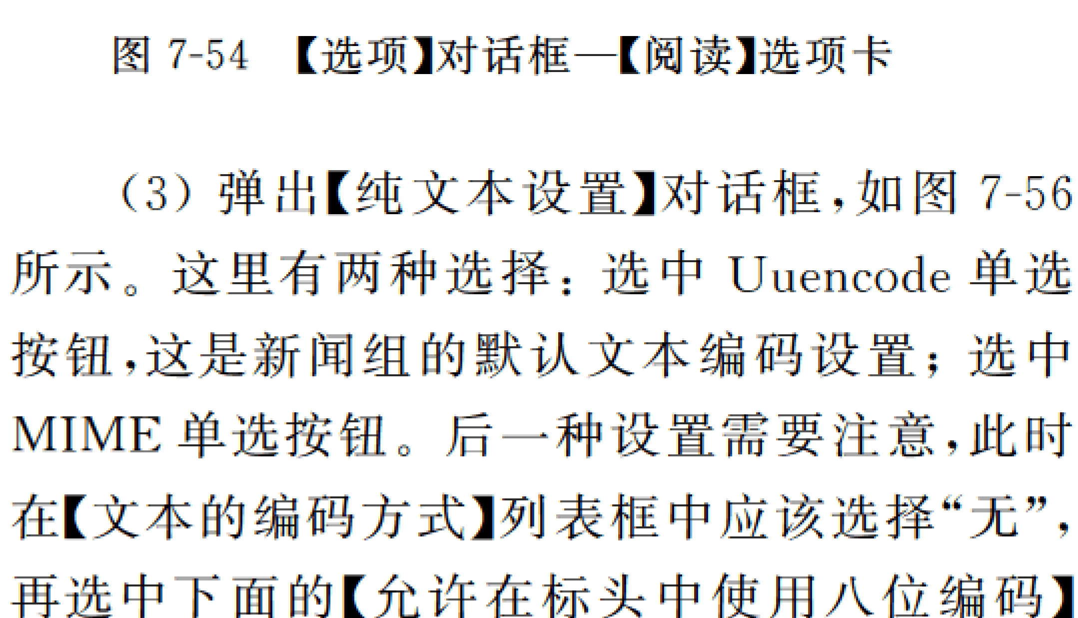


图 7-55　【选项】对话框—【发送】选项卡



(3) 弹出【纯文本设置】对话框，如图 7-56 所示。这里有两种选择：选中 Uuencode 单选按钮，这是新闻组的默认文本编码设置；选中 MIME 单选按钮。后一种设置需要注意，此时在【文本的编码方式】列表框中应该选择“无”，再选中下面的【允许在标头中使用八位编码】复选框。



图 7-56　【纯文本设置】对话框



(4) 在 Outlook Express 中选择【查看】→【当前视图】→【显示所有邮件】命令和【按对话分组邮件】命令。

(5) 在 Outlook Express 中选择【查看】→【排序方式】→【发送时间】命令和【降序】命令。

(6) 设定新闻组规则

① 规则＃1：跟踪别人对自己帖子的回复。

在 Outlook Express 中选择【工具】→【邮件规则】→【新闻】命令，会弹出【新建新闻规则】对话框。按下述步骤进行设置，设置后的界面如图 7-57 所示。

在【1. 选择规则条件】选项区域中，选中【若“发件人”行中包含用户】复选框。

在【2. 选择规则操作】选项区域中，选中【将邮件标记为被跟踪或忽略】复选框。

在【3. 规则描述】选项区域中进行编辑。单击【包含‘NewsGroupTest’】超级链接，出现了新对话框，按上面的要求，输入网名或昵称(这里输入之前设置的 NewsGroupTest)，然后单击【添加】按钮，再单击【确定】按钮后返回【新建新闻规则】对话框。

在【3. 规则描述】选项区域中进行编辑。单击【被监测】超级链接，在弹出的对话框中选中【跟踪邮件】单选按钮，单击【确定】按钮后返回【新建新闻规则】对话框。再单击【确定】按钮退出。

② 规则＃2：避免下载体积过大的新闻帖子。

在 Outlook Express 中选择【工具】→【邮件规则】→【新闻】命令，会弹出【新建新闻规则】对话框。按下述步骤进行设置，设置后的界面如图 7-58 所示。



在【1. 选择规则条件】选项区域中，选中【若邮件中的行数超过行】复选框。

在【2. 选择规则操作】选项区域中，选中【将邮件标记为被跟踪或忽略】复选框。



图 7-57 【新建新闻规则】对话框—规则#1



图 7-58 【新建新闻规则】对话框—规则#2

在【3. 规则描述】选项区域中进行编辑。单击【行】超级链接，出现新对话框。在对话框的【行数】上下控件中输入500(这是最常见的设置数)，再单击【确定】按钮则返回【新建新闻规则】对话框。

在【3. 规则描述】选项区域中进行编辑。单击【被忽略】超级链接，在弹出的对话框中选中【忽略邮件】单选按钮，单击【确定】按钮后返回【新建新闻规则】对话框。再单击【确定】按钮退出。

7.4.3 发表和回复新闻组文件

发表和回复新闻组文件的具体操作步骤如下：

(1) 在Outlook Express中选择【文件】→【新建】→【新闻邮件】命令，如图7-59所示。

(2) 此时弹出【撰写新邮件】窗口，如图7-60所示。向新闻组group.chapter7写一封信，信的主题为News Test，内容为“This is only a test!”。

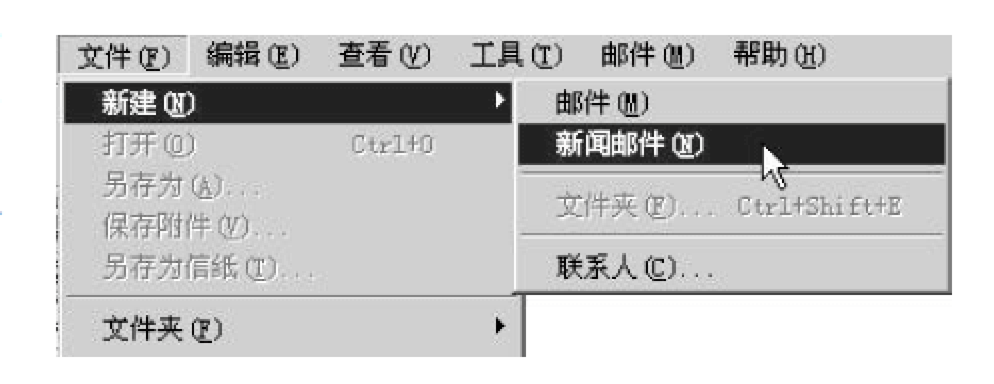


图 7-59 Outlook Express 的【文件】菜单

(3) 单击【发送】按钮，信件成功发送。此时弹出【张贴新闻】对话框，如图7-61所示。选中【不再显示此信息】复选框，单击【确定】按钮。

(4) 此时查看新闻组group.chapter7账户，可以看到收到一封新邮件，查看其内容正是之前发送的邮件，如图7-62所示，表明向新闻组发表文件成功。

(5) 测试回复功能。选择刚收到的邮件，单击Outlook Express工具栏中的【答复组】按钮，此时弹出回复邮件窗口，如图7-63所示。向新闻组group.chapter7回复邮件，邮件主题采用默认值Re:News Test，内容为“新闻组测试成功!”。然后单击【发送】按钮，信件成功发送。







图 7-60 【撰写新邮件】窗口



图 7-61 【张贴新闻】对话框



图 7-62 查看新闻组邮件



图 7-63 回复新闻组邮件



（6）此时再查看新闻组 group. chapter7 账户，界面如图 7-64 所示，表明向新闻组回复文件成功。另外还可以看出，回复的帖子都用红色字体显示，表明此前设置的新闻组规则发挥了作用。



图 7-64　查看新闻组邮件

（7）在局域网内另一台机器上，使用 a@test. com 账户向新闻组发表文件，其中一封邮件带有附件，均成功完成。此时再查看新闻组 group. chapter7 账户，界面如图 7-65 所示，表明 DNews 新闻组服务器工作正常。

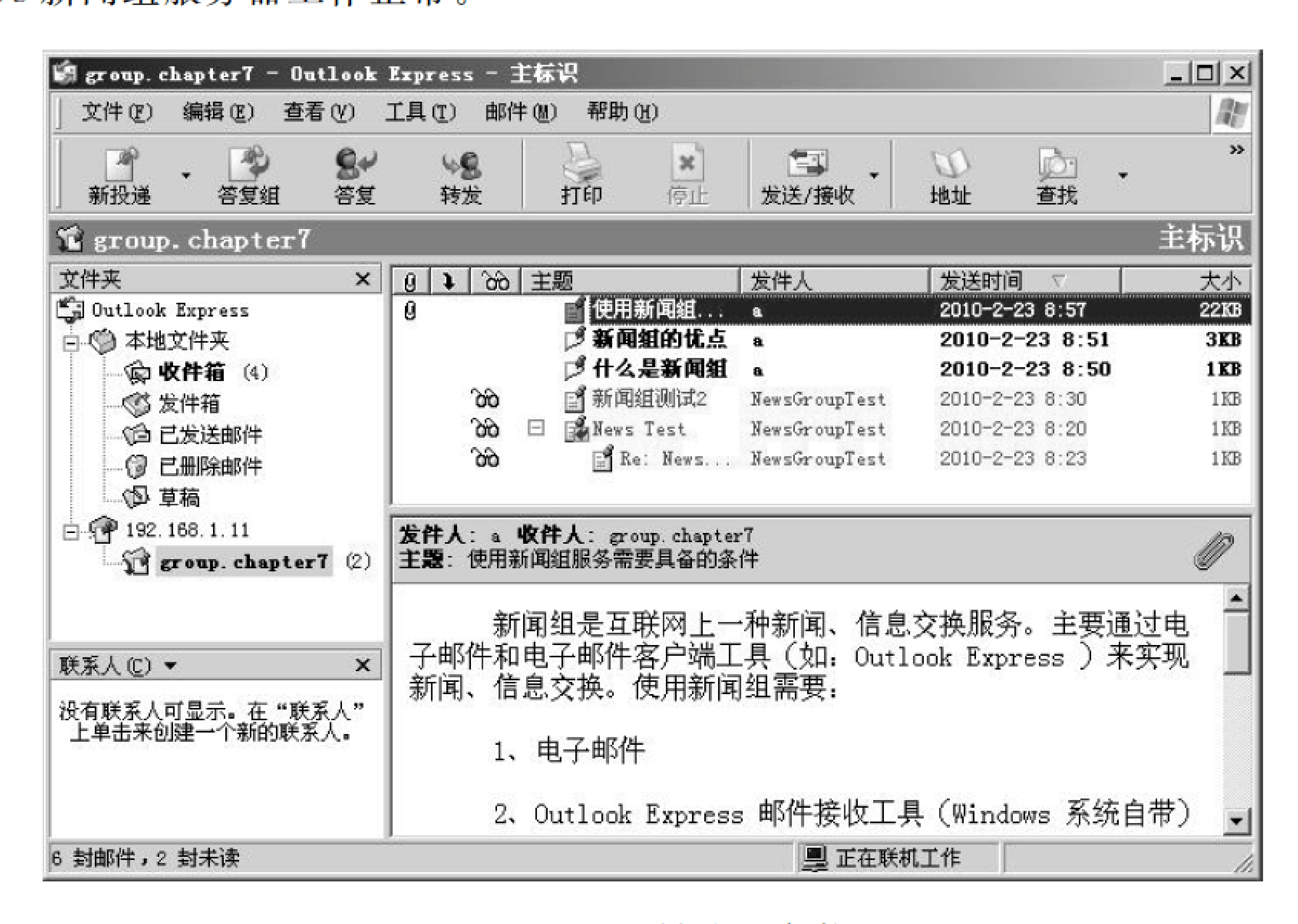


图 7-65　查看新闻组邮件



7.5　疑难解答

（1）常见的新闻组服务器类型有哪些？

新闻组的类型有很多，其中，热门的 Usenet 新闻组主要有 comp（计算机科学及相关的话题）、news（一般性的新闻话题）、rec（个人爱好、娱乐活动、艺术话题）、sci（科学研究、工程技术）、soc（社会类话题）、biz（商业类话题）、talk（有争议的话题）、misc（不属于以上几类的或有交叉的话题）、alt（各类话题）等。

（2）如何配置 DNews 服务器的过期规则？

随着新闻组用户日益增多，服务器上的新闻条目也会越来越多，会占用大量的磁盘空间，影响系统运行效率。此时可以通过设置过期规则来限制新闻的保存，并自动删除过期新闻。具体操作步骤如下：

① 在 DNews 5.7e1 Admin Tool 管理工具窗口的菜单栏中选择 Configure→Expire Rules 命令，会弹出 Expire Rules 对话框。此时已经定义的规则会在左侧列表框中列出，可以双击进行编辑。如果要定义新的规则，则单击左下侧的 Add Pile 按钮。

② 此时会弹出 Expire Rules for a specific Pile 对话框，如图 7-66 所示。从中即可进行相关设置，具体设置选项如下：

- Max percentage of disk space for these groups 列表框。设置该新闻组占用磁盘空间的最大百分比。
- Max days to store items in these groups 列表框。设置该新闻组新闻条目保留的最大天数。
- Sort buckets to improve reader speed 复选框。设置是否对新闻条目进行排序以提高读取效率。
- Groups 列表框。设置过期规则适用的新闻组范围。
- Days to store history records after items are expired 列表框。设置新闻条目过期后，相应的历史记录保存的天数。

输入完毕之后，单击 OK 按钮完成设置。

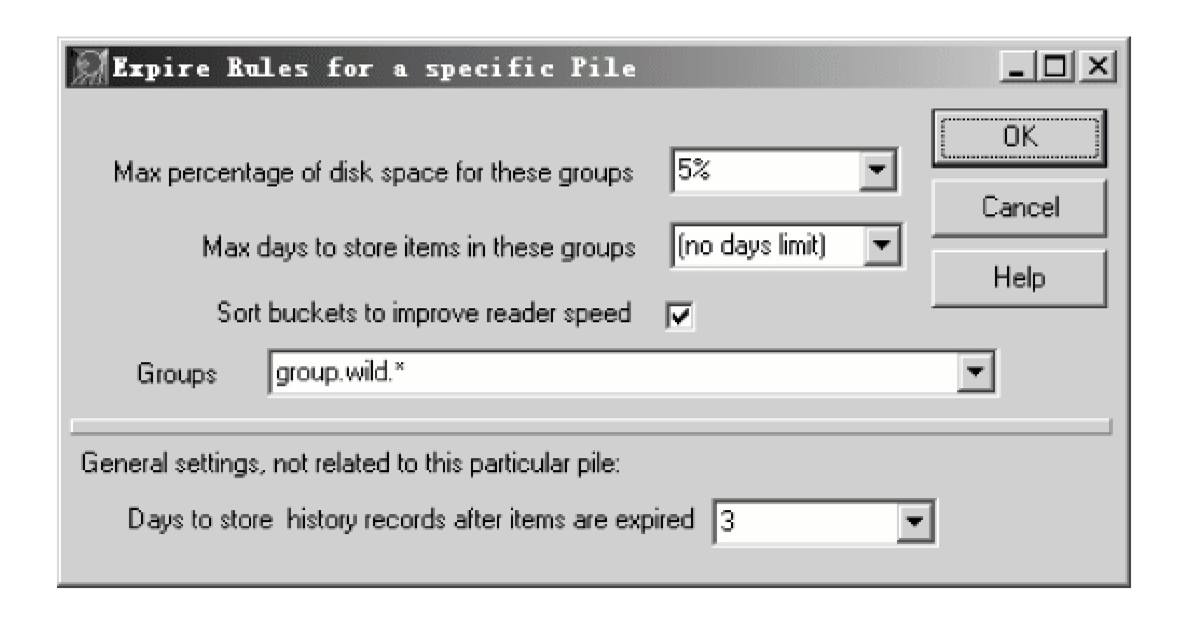


图 7-66　Expire Rules for a specific Pile 对话框

（3）磁盘空间不足，如何将缓存文件目录移动到别的磁盘？

假设 DNews 安装在 C:\dnews\目录，由于 C 盘空间不足，需要将缓存目录 C:\dnews\



spool 移动到 D:\dnews\spool。具体的操作步骤如下:

① 停止 DNews 的运行。

② 将整个 spool 文件目录移动到新位置。

③ 编辑 dnews.conf 文件(C:\windows\system32\dnews.conf),将其中的语句 spool C:\dnews\spool 修改为 spool D:\dnews\spool。

④ 重新启动 DNews。

(4) 如何使用 telnet 命令测试 DNews 服务器是否正常运行?

NNTP 是基于文本的协议,所以可以不必借助如何软件,使用 telnet 命令手工测试新闻服务器,甚至是阅读新闻。具体的操作步骤如下:

① 在【命令提示符】窗口输入 telnet feeder.site 119,远程登录服务器。

② 登录成功后,依次输入以下命令来测试服务器:

- mode reader(该命令定义操作模式为阅读新闻模式)。
- group 新闻组名称(该命令选择一个新闻组,例如 group.test)。
- head(该命令显示新闻标题)。
- body(该命令显示新闻正文)。
- next(该命令显示下一条新闻)。
- help(该命令显示有效的操作命令)。
- quit(该命令中断远程连接)。

习　　题

1. 填空题

(1) 新闻组服务器与客户端程序是采用________协议,使用的端口号是________。

(2) DNews 的安装模式有三种,分别是________、________和________。

2. 选择题

(1) DNews 支持的操作系统包括(　　)。

A. Windows　　B. Linux　　C. Solaris　　D. AIX

(2) DNews 提供了三种方式对新闻组服务器进行配置和管理,分别是(　　)。

A. 图形界面　　B. 命令行

C. 超级管理员　　D. 基于 Web 的远程管理

3. 思考题

(1) 简述新闻发布和接收的流程。

(2) 在 Outlook Express 中发送和接收新闻邮件和普通电子邮件有何异同?

4. 上机题

使用浏览器,在远程创建一个名为 chapter7test 的新闻组账户。





第8章　流媒体服务

本章要点

- 了解流媒体的基础知识
- 掌握 Windows Media 服务的安装和基本配置
- 掌握如何使用 Windows Media 提供点播服务

作为新一代互联网应用的标志，流媒体技术在近几年得到了飞速的发展。由于其自身的优越性，流媒体技术被广泛应用于视频点播、视频会议、远程教育、远程医疗和网络电视(IPTV)等领域。

8.1　流媒体概述

8.1.1　流媒体的概念

流媒体(Streaming Media)是一种以音视频数据流的方式在网络上传递多媒体信息的技术。与传统的多媒体下载不同，流媒体传输具有实时性和连续性的特点。

如图 8-1 所示，流式传输时，声音、影像或动画等多媒体信息由流媒体服务器向流媒体客户机连续、实时传送。它首先在客户端的计算机上创建一个缓冲区，于播放前预先下载一段资料作为缓冲，用户不必等到整个文件全部下载完毕，而只需经过几秒或数十秒的启动延时即可进行观看。当多媒体信息在客户机上播放时，文件的剩余部分将在后台从服务器内继续下载。如果网络连接速度小于播放的多媒体信息需要的速度，播放程序就会取用先前建立的一小段缓冲区内的资料，避免播放的中断，使得播放品质得以维持。

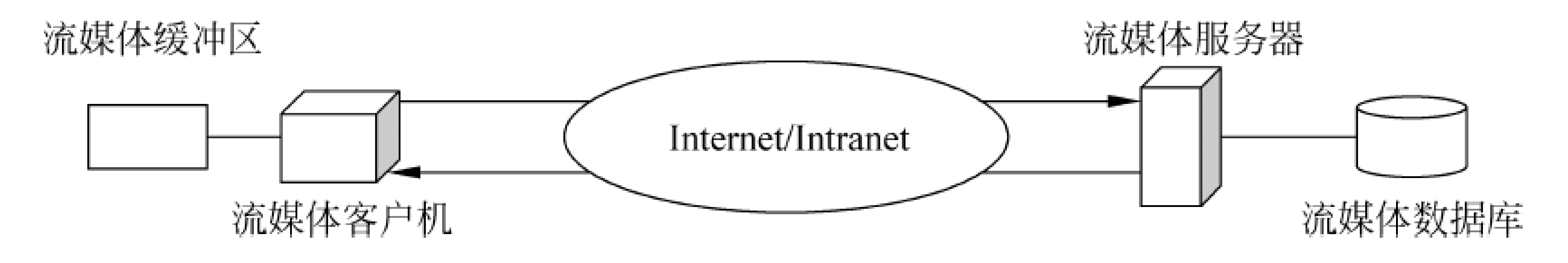


图 8-1　流媒体服务的原理

流式传输除了能够发送已经制作完成的文件外，还可以通过采集服务器实时采集现场音视频，推送到流媒体服务器端，实时提供给用户。因此，流媒体除了能够更好地承担如下



载一样的多媒体点播服务外，更能够应用在现场直播、电视转播、突发事件报道等多种对实时性传输要求较高的领域。

8.1.2 流式播放方式

1. 单播

单播是指在客户端与媒体服务器之间建立一个单独的数据通道，从一台服务器送出的每个数据包只能传送给一个客户机。每个用户必须分别对媒体服务器发送单独的请求，而媒体服务器必须向每个客户机发送所申请的数据包复制。这种巨大冗余首先造成服务器沉重的负担，响应需要很长时间，甚至停止播放；管理人员也需被迫购买硬件和带宽来保证一定的服务质量。

2. 组播

IP组播技术构建了一种具有组播能力的网络，允许路由器一次将数据包复制到多个通道上。采用组播方式，单台服务器能够对几十万台客户机同时发送连续数据流而无延时。媒体服务器只需要发送一个信息包，而不是多个；所有发出请求的客户端共享同一信息包。信息可以发送到任意地址的客户机，减少网络上传输的信息包的总量。网络利用效率大大提高，成本大为降低。

3. 点播与广播

点播指的是客户端与服务器之间的主动连接。在点播连接中，客户端发出选择节目内容的请求，服务器响应客户端请求将节目内容传输给客户端。客户端可以开始、停止、后退、快进或暂停流。点播连接提供了对流的最大控制，但这种方式由于每个客户端各自连接服务器，从而会迅速消耗大量网络带宽。

广播指的是客户端被动接收流。在广播过程中，客户端接收流，但不能控制流。例如，客户端不能暂停、快进或后退该流。广播方式中数据包的单独一个备份将发送给网络上的所有客户端，而不管客户端是否需要，从而造成网络带宽的浪费。

提示：在实际应用中，播放方式一般将上述方式结合起来，如点播单播、广播单播和广播多播。

8.1.3 流媒体传输方式

流式传输是流媒体实现的关键技术，根据实现原理可分为顺序流传输（Progressive Streaming）和实时流传输（Realtime Streaming）。

1. 顺序流传输

顺序流传输采用顺序下载的方式进行传输，在下载的同时用户可以在线回放多媒体数据，但给定时刻只能观看已经下载的部分，不能跳到尚未下载的部分，也不能在传输期间根



据网络状况对下载速度进行调整。由于标准的 HTTP 服务器即可实现顺序发送，而不需要其他特殊协议支持，因此经常被称作 HTTP 流式传输。

顺序流式传输的优点：

- 支持无损下载，能够保证播放的最终质量；
- 由标准的 HTTP 协议支持，兼容性好，不受防火墙的影响。

顺序流式传输的缺点：

- 不支持随机访问；
- 对于慢速连接来说，相应的延迟也比较严重；
- 不支持现场直播。

因此，顺序流传输方式适合传送较高质量的短片段多媒体内容，如片头、片尾和广告等。

2. 实时流传输

实时流传输保证媒体信号带宽能够与当前网络状况相匹配，从而使得流媒体数据总是被实时地传送，因此特别适合于现场事件。实时流传输支持随机访问，即用户可以通过快进或者后退操作来观看前面或者后面的内容。从理论上讲，实时流媒体一经播放就不会停顿，但事实上仍有可能发生周期性的暂停现象，尤其是在网络状况恶化时更是如此。与顺序流传输不同的是，实时流传输需要用到特定的流媒体服务器，而且还需要特定网络协议的支持。

实时流式传输的优点：

- 支持真正的实时传输；
- 支持现场直播；
- 支持随机访问。

实时流式传输的缺点：

- 有损下载，使用慢速连接时的播放质量较差；
- 穿过防火墙时有时会出现问题；
- 需要专门的服务器和协议支持，配置和管理更为复杂。

因此，实时流传输特别适合实时播放的需要，如现场直播等。

8.1.4　流媒体的传输协议

1. 实时传输协议(RTP、RTCP)

RTP(Real-time Transport Protocol)是用于 Internet 上针对多媒体数据流的一种传输协议。RTP 被定义为在一对一或一对多的传输情况下工作，其目的是提供时间信息和实现流同步。通常使用 UDP 来传送数据，但也可工作在 TCP 或 ATM 等协议之上。RTP 本身并不能为按顺序传送数据包提供可靠的传送机制，也不提供流量控制或拥塞控制，而是依靠 RTCP 提供这些服务。

RTCP(Real-time Transport Control Protocol)与 RTP 共同提供流量控制和拥塞控制服务。在 RTP 会话期间，参与者周期性地传送 RTCP 包，这些包中含有已发送数据包的数



量、丢失数据包的数量等统计数据，服务器可根据这些信息动态地改变传输速率，甚至改变有效载荷类型。RTP 与 RTCP 的配合使用，能以有效的反馈和最小的开销使传输效率最佳化，非常适合传送网上的实时数据。

2. 资源预留协议(RSVP)

资源预留协议(Resourcere Ser Vation Protocol，RSVP)是针对 IP 网络传输层不能保证 QoS 和支持多点传输而提出的协议。使用 RSVP 预留一定的网络资源，建立静态或动态的传输逻辑通路，从而保证每一业务流都有足够的“独享”带宽，因而能够克服网络的拥塞和丢包，提高 QoS 性能。

3. 实时流协议(RTSP)

RTSP(Real-Time Streaming Protocol)是由 RealNetworks、Netscape 共同提出的一种协议，它定义了如何使一对多应用程序有效地通过 IP 网络传送多媒体数据。RTSP 在体系结构上位于 RTP、RTCP 之上，它使用 TCP 或 RTP 完成数据传输。与 HTTP 相比，RTSP 传送的是多媒体数据，而 HTTP 传送 HTML。在使用 RTSP 时，客户机和服务器均可发出请求。也就是说，RTSP 可双向服务，而 HTTP 的请求是由客户机发出，服务器进行响应。

提示：在流媒体传输中，标准的协议就是 RTP(实时传输协议)、RTCP(实时传输控制协议)、RSVP(资源预留协议)和 RTSP(实时流协议)，厂商们的产品都是在这些协议的基础上进行研究与开发。限于篇幅，这里不再深入讨论。

8.1.5 流媒体的文件格式

目前流媒体领域有三大生产厂商，包括 RealNetworks 公司、Microsoft 公司和 Apple 公司。这些公司推出的流媒体文件格式较多，下面仅介绍一些常用的格式。

1. ASF

ASF(Advanced Streaming Format，高级流媒体格式)是微软公司开发的一种使用了 MPEG-4 压缩算法的可以在网上实时观看的流媒体格式。它的使用与 Windows 操作系统是分不开的，其播放器 Microsoft Media Player 已经与 Windows 捆绑在一起，不仅用于 Web 方式播放，还可以在浏览器以外的地方播放影音文件。

2. WMV

WMV(Windows Media Video，Windows 媒体视频)是微软在 ASF 基础上推出的一种媒体格式，具有体积小、可进行高速网络传输等特点。目前，在网络上比较流行。通过 Windows Media Encoder 软件可制作 WMV 和 ASF 文件。

3. AVI

AVI 是音频视频交错(Audio Video Interleaved)的英文缩写。AVI 这个由微软公司从





Win3.1时代就开始发表的旧视频格式，兼容性好，调用方便，图像质量好。但缺点是文件体积过于庞大。也正是由于这个原因，后来陆续有MPEG-1和现在MPEG-4的出台。

4. MPEG

MPEG(Moving Picture Experts Group，运动图像专家组标准)是一种从数字音频和视频发展起来的压缩编码标准，包括MPEG音频、MPEG视频和MPEG系统三个部分。在多媒体数据压缩标准中，采用比较多的MPEG标准有MPEG-1(VCD采用该标准)、MPEG-2(DVD采用该标准)和MPEG-4。常见的MP3和MPG两种格式就是MPEG的一种典型应用。

5. RM、RA和RMVB

RM(Real Media)和RA(Real Audio)格式是RealNetworks公司开发的一种流媒体文件格式，主要用来在低速率的网络上实时传输活动视频影像，可以根据网络数据传输速率的不同而采用不同的压缩比率，在数据传输过程中边下载边播放视频影像，从而实现影像数据的实时传送和播放。RMVB中的VB是指Variable Bit Rate(可变比特率，简称VBR)，该格式使用了更低的压缩比特率，这样制成的文件体积更小，而且画质并没有太大的变化。

6. MOV

MOV是Apple公司开发的一种流媒体文件格式。MOV早期使用在MAC机上，如今可以在Windows中使用QuickTime等播放器来播放该类型的文件。

7. SWF

SWF是基于Macromedia公司Shockwave技术的流媒体动画格式，是用Flash软件制作的一种格式，源文件为.fla格式。由于其体积小、功能强、交互能力好、支持多个层和时间线程等特点，因此越来越多地应用到网络动画中。SWF文件是Flash的其中一种发布格式，已广泛用于Internet上，客户端安装Shockwave的插件即可播放。

8.1.6 流媒体应用系统的组成

流媒体是由各种不同的互相通信交互的软件系统构成的，模块之间通过特定的协议互相通信，并按照特定格式互相交换文件数据。一个最基本的流媒体系统包含编码器(Encoder)、服务器(Server)、播放器(Player)三个组件。

如图8-2所示，客户端通过流媒体播放器观看流媒体文件，作为发送流媒体的服务器接受客户端发出的播放该文件的请求。此时，编码器将服务器上的这一文件进行编码。

编码器对原始的音视频媒体源进行一定格式的压缩编码，将其转化为流格式，以便在网络上传播。编码过程包括两项工作。一是尽可能在保证原有声音影像质量的情况下，降低文件的数据量；二是按照容错格式将转换后的文件打包，这种处理方式能够避免数据传输时发生丢失。

文件在编码后被存放在流媒体服务器上。流媒体服务器主要完成以下工作：



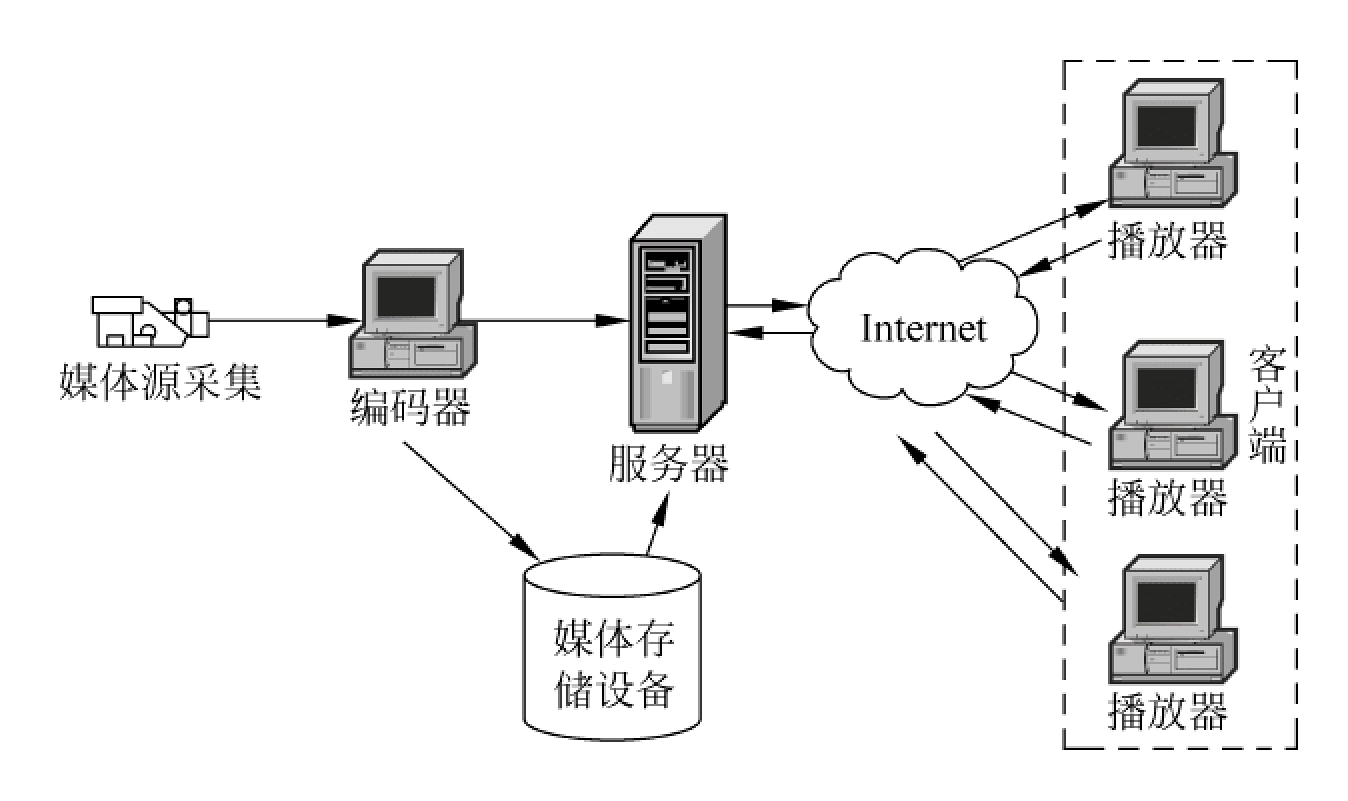


图 8-2　流媒体系统基本结构

(1) 响应客户的请求,把媒体数据传送给客户。流媒体服务器在流媒体传送期间必须与客户的播放器保持双向通信。这种通信是必需的,因为客户可能随时暂停或快放一个文件。

(2) 响应广播的同时能够及时处理新接收的实时广播数据,并将其编码。

(3) 可提供其他额外功能,如数字权限管理(DRM)、插播广告、分割或镜像其他服务器的流,还有组播。

流媒体播放器是一种能够与流媒体服务器通信的软件,可以播放或丢弃收到的流媒体文件。流媒体播放器中提供对流的交互式操作,如播放、暂停、快放等。某些播放器还提供一些额外功能,如录制、调整音频或视频等。目前,被广泛使用的播放器主要有 RealNetworks 公司的 Real Player、Microsoft 公司的 Windows Media Player 和 Apple(苹果)公司的 Quicktime 播放器。

8.2　Windows Media 服务的安装和基本配置

流媒体服务器是流媒体应用的核心系统,是向客户端提供视频服务的关键平台。流媒体应用系统的主要性能体现都取决于媒体服务器的性能和服务质量。因此,流媒体服务器是流媒体应用系统的基础,也是最主要的组成部分。

作为 PC 操作系统的龙头,微软借助其操作系统平台优势,从 Windows 2000 服务器开始,推出了 Windows Media 服务,提供了一种业界领先、具有极强伸缩性和扩展性的媒体服务器解决方案,从具有数百个连接请求的小型 Internet 电台到生成数百万个请求的大规模的流式媒体网站,都可使用它。

8.2.1　Windows Media 服务的安装

要使用 Windows Media 提供流媒体服务,必须首先安装 Windows Media 服务。默认情况下,Windows Server 2003 没有安装 Windows Media 服务。可使用【配置您的服务器向导】工具来安装流式媒体服务器,也可通过【控制面板】进行安装。具体的操作步骤如下:

(1) 依次选择【开始】→【控制面板】→【添加/删除程序】,打开如图 8-3 所示的【添加或



删除程序】窗口。单击【添加/删除 Windows 组件】图标，打开如图 8-4 所示的【Windows 组件向导】对话框。

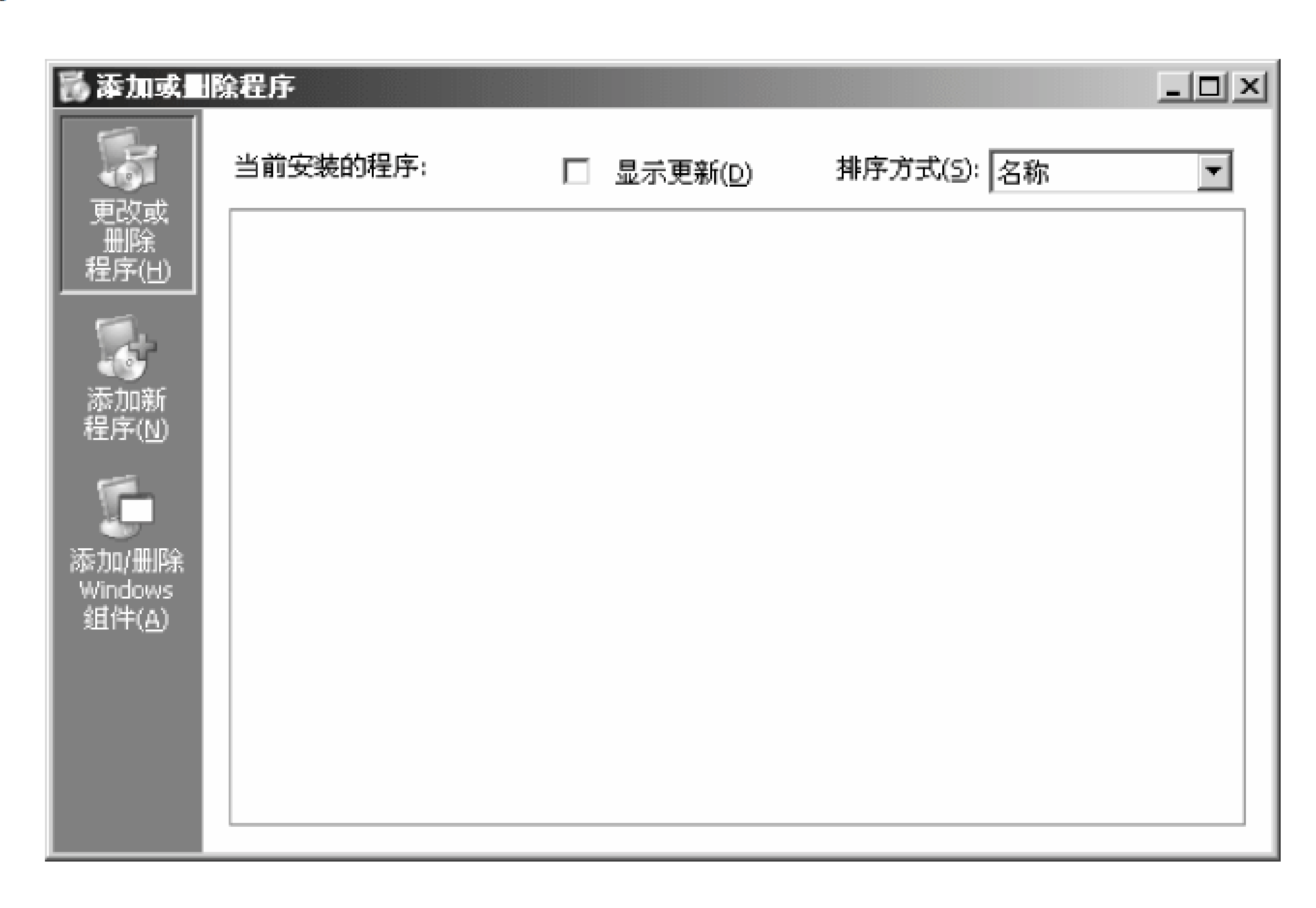


图 8-3　【添加或删除程序】窗口

（2）在【组件】列表中，双击 Windows Media Services 组件，打开组件详细选项的对话框，如图 8-5 所示。

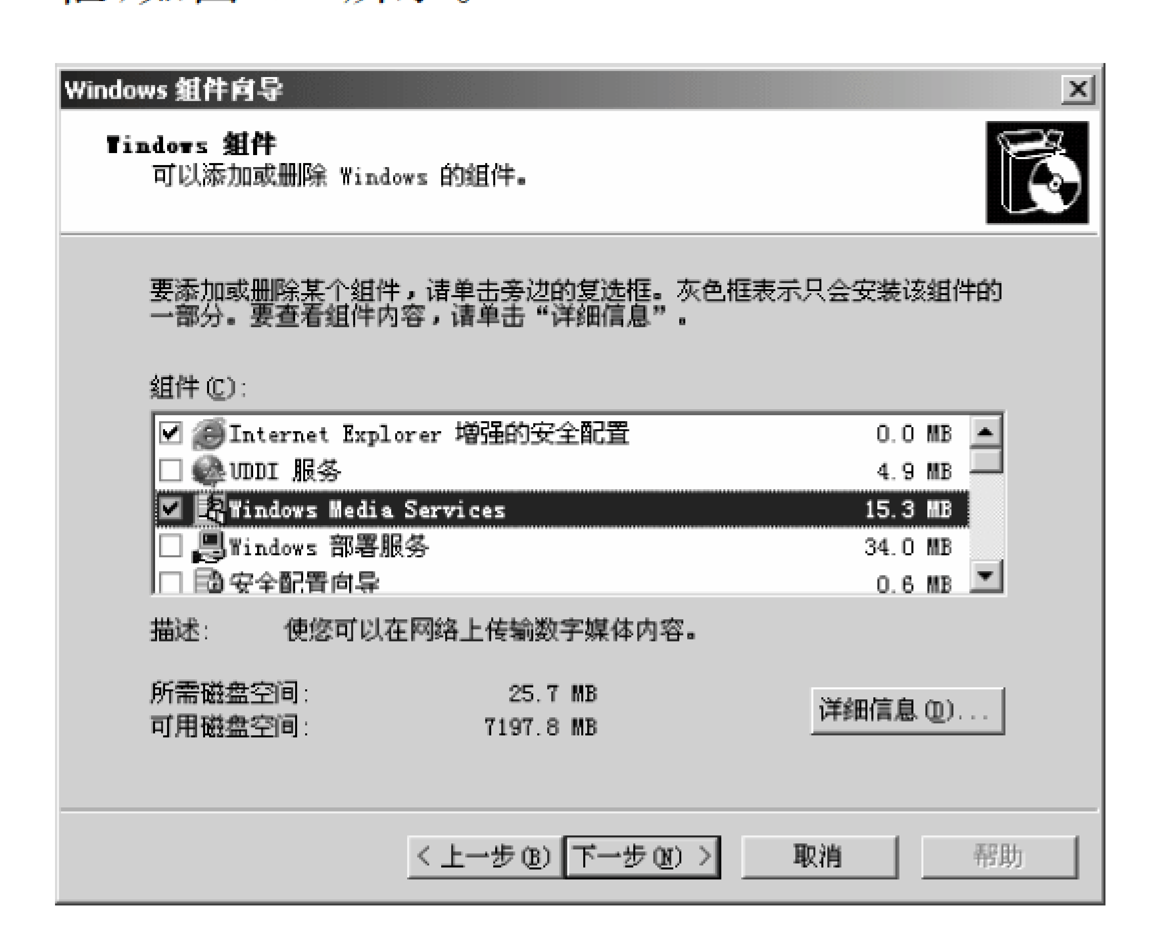


图 8-4　【Windows 组件向导】对话框



图 8-5　选择媒体服务组件详细选项

（3）选择详细的组件选项。默认情况下，Windows Media Services 和【Windows Media Services 管理单元】复选框被选中。如果要使用浏览器进行远程管理，应选中【用于 Web 的 Windows Media Services 管理器】复选框，自动创建一个 IIS 的 Windows Media Services 管理站点。如果选中【多播和广告日志记录代理】复选框，就会记录通过 Web 服务器连接到内容的客户机的统计信息，需要 IIS 6.0 支持。这两个选项可以根据管理员的需要决定是否安装。单击【确定】按钮，返回组件向导。

（4）在【Windows 组件向导】对话框中，单击【下一步】按钮，系统开始安装所选组件。在此过程中系统将提示插入系统安装光盘，如图 8-6 所示。

（5）将系统安装光盘放入光驱中，单击【确定】按钮，系统将继续自动安装所有所选组



件。等到出现如图 8-7 所示的【完成“Windows 组件向导”】对话框时，单击【完成】按钮。至此，服务器安装完毕。



图 8-6　提示插入系统安装光盘



图 8-7　【完成“Windows 组件向导”】对话框

8.2.2　Windows Media 服务器级的基本设置

Windows Media 服务器的设置主要包括属性、插件、发布点和服务器端播放列表，服务器级的设置应用于该服务器上的所有发布点。这里主要介绍一下服务器级的属性和插件的基本设置。属性用于设置适用于 Windows Media Services 的基本规则，可将属性应用于整个服务器，也可应用于特定的发布点。插件用于提供额外的功能，如日志记录、验证、数据源和控制协议，可将插件应用到整个 Windows Media 服务器，也可应用到特定的发布点。具体的操作步骤如下：

（1）依次选择【开始】→【管理工具】→Windows Media Services，进入 WMS 管理控制台，如图 8-8 所示。



图 8-8　WMS 管理控制台



（2）选中要管理的服务器，在右侧窗格中选择【属性】选项卡，如图 8-9 所示。则左下侧显示插件类别，右下侧显示该类别的所有属性或插件。下面简单介绍几个属性（或插件）的设置。



图 8-9　【属性】选项卡

- 在【类别】列表中单击【限制】项，则在右侧窗格中为连接参数设置限制，以精确地管理服务器资源，如图 8-10 所示。



图 8-10　设置限制

- 在【类别】列表中单击【控制协议】项，则右侧窗格中显示 3 个插件，如图 8-11 所示。默认情况下，启用了 MMS 和 RTSP 两种协议。要启用 HTTP 协议，应将【WMS HTTP 服务器控制协议】的状态变为启用。还可以为每个插件设置属性，如双击【WMS MMS 服务器控制协议】，打开相应的对话框，从中可进一步设置该协议的 IP 地址和端口，如图 8-12 所示。
- 在【类别】列表中单击【数据源】项，则在右侧窗格中显示 4 个数据源插件，如图 8-13 所示。数据源插件支持 Windows Media Services 读取来自不同渠道的数据。





图 8-11 设置控制协议



图 8-12 设置 WMS MMS 服务器控制协议属性



图 8-13 设置数据源





8.3　使用 Windows Media 提供点播服务

搭建好 Windows Server 2003 的视频服务器后，就可以使用它来进行视频和音频点播。Windows Media 服务提供了建立点播服务器的简便方法，管理员可以通过创建不同的发布点来建立点播和广播服务。服务器安装完毕时已经配置了两个对应点播和广播服务的发布点，但管理员往往需要自定义的发布点。下面介绍如何新建一个点播发布点。

8.3.1　创建发布点

在本例中，将使用向导创建一个名为“点播 1”的发布点。这个发布点指向 E 盘的“点播 1”文件夹，在“点播 1”文件夹中存有事先做好的 WMS 文件。

具体的操作步骤如下：

(1) 依次选择【开始】→【管理工具】→Windows Media Services，进入 WMS 管理控制台。展开左侧控制台树，右击【发布点】选项，并在弹出的如图 8-14 所示的快捷菜单中选择【添加发布点(向导)】命令，将打开如图 8-15 所示的【添加发布点向导】对话框。

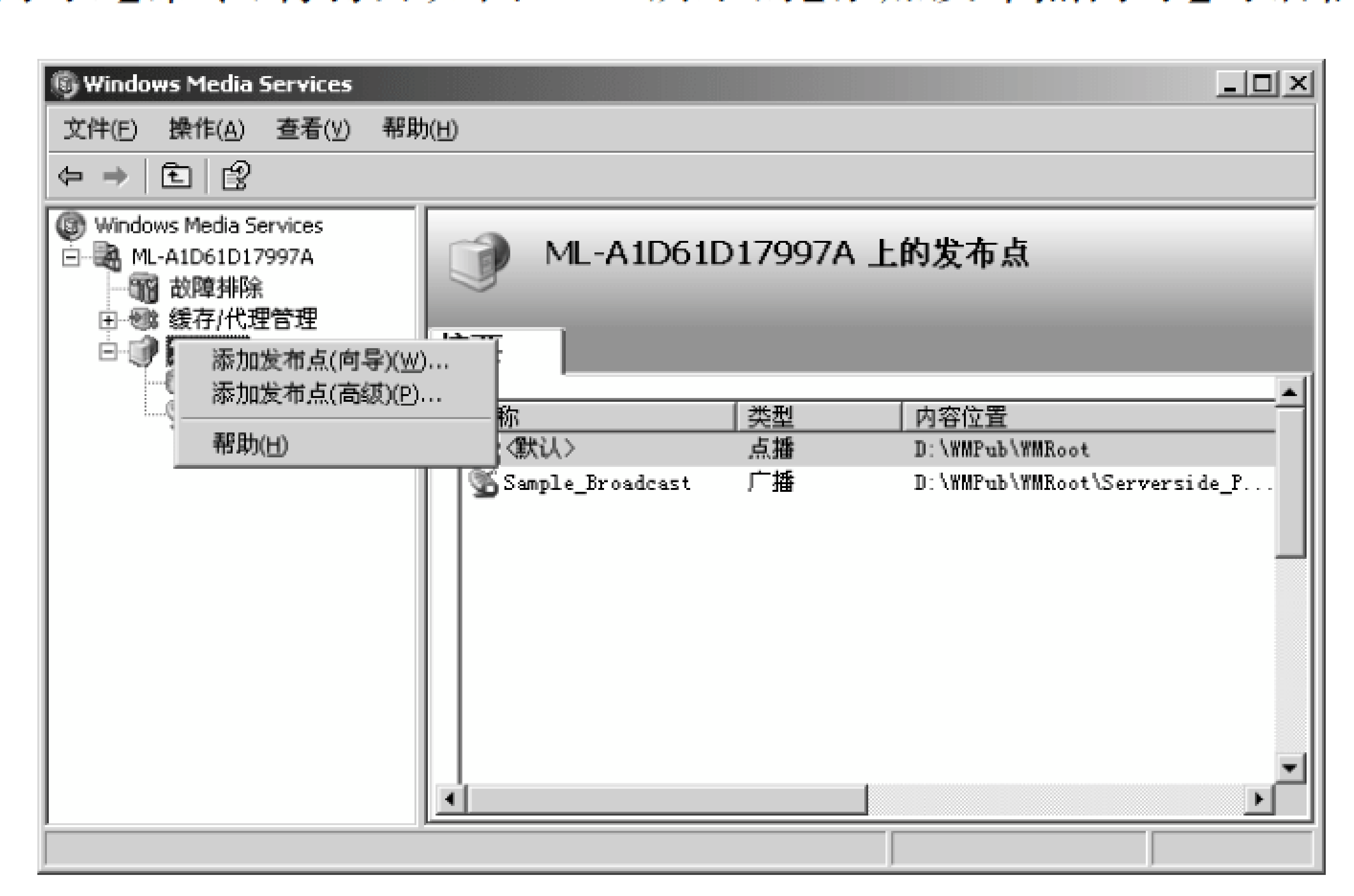


图 8-14　在 WMS 中添加发布点

(2) 单击【下一步】按钮，将显示【发布点名称】对话框，如图 8-16 所示。在【名称】文本框中输入该发布点的名称，其默认值为 PublishingPoint1。为了更方便其他用户识别，也可以修改成其他名称。本例中输入“点播 1”。

(3) 单击【下一步】按钮，打开如图 8-17 所示的【内容类型】对话框，选择发布的内容类型。对于点播发布点，一般选择【一个文件】或【目录中的文件】单选按钮。在此选择



图 8-15　【添加发布点向导】对话框



【目录中的文件】单选按钮。

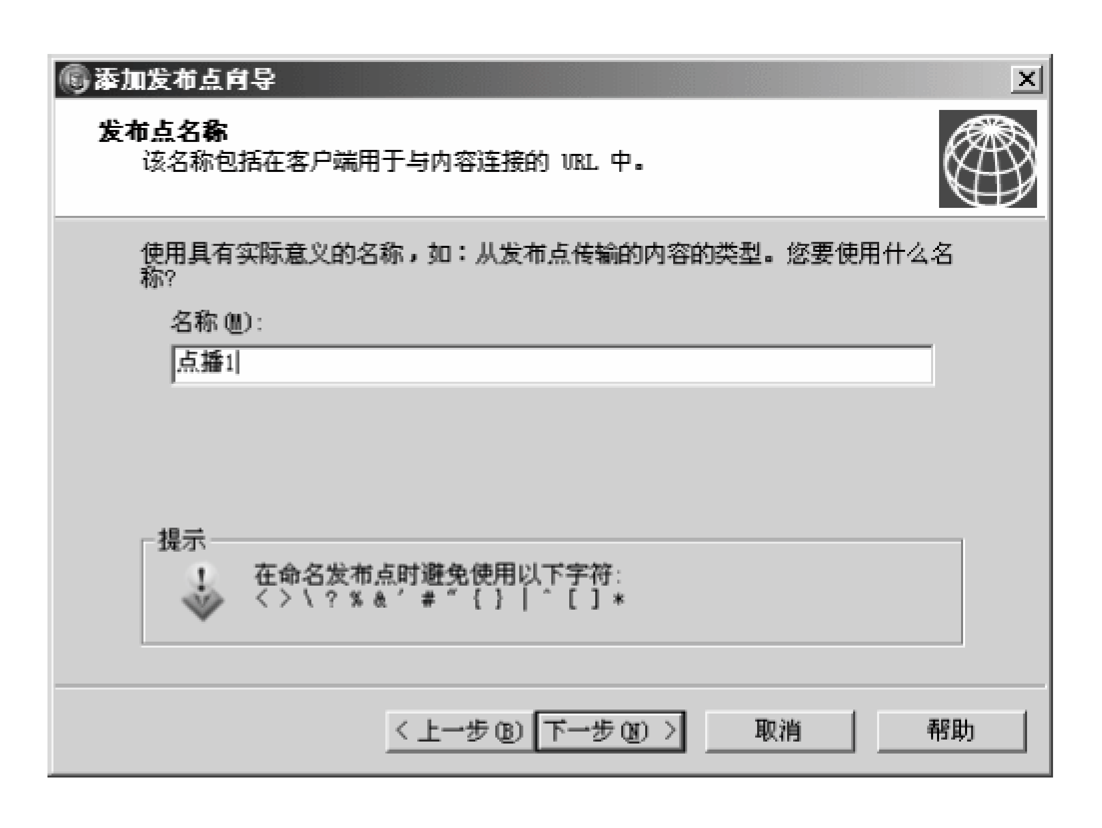



图 8-16 【发布点名称】对话框



图 8-17 【内容类型】对话框

提示：编码器(实况流)：该单选按钮使服务器连接到编码计算机上，然后广播由编码器所创建的流。由于它的内容不是 Windows Media 文件，所以通常将它称为实况流。编码器正在创建的内容可以源自录像带、DVD、.avi 文件或诸如照相机或麦克风之类的实况源。这种类型仅适用于广播发布点，所以在建立点播时不能选择该单选按钮。

播放列表：该单选按钮可以创建一个能够添加一个或多个流文件的发布点，以用于传输一系列在播放列表中已指定的内容。

一个文件：该单选按钮使用发布点来传输单个文件。默认情况下，Windows Media 服务可以传输具有如下文件扩展名的文件：.wma、.wmv、.asf、.wsx 和.mp3 等。

目录中的文件：该单选按钮适用于通过单个发布点来实现点播的播放，以使发布点传输多个内容。通过将文件名包括在 URL 中来请求单个文件，或者按顺序传输目录中的所有文件，客户端可以访问指定文件夹中的所有文件。

(4) 单击【下一步】按钮，打开如图 8-18 所示的【发布点类型】对话框，选择发布点类型。这里选择【点播发布点】单选按钮，以创建点播发布点。

(5) 单击【下一步】按钮，打开【目录位置】对话框。在这里可以指定该点播发布点主目录所在文件夹。如果在创建的点播发布点中要按次序传输该目录下的所有文件，就应当选择【允许使用通配符对目录内容进行访问】复选框。在本例中应通过【浏览】按钮选择"E:\点播 1"，并且选中【允许使用通配符对目录内容进行访问】复选框，如图 8-19 所示。

(6) 单击【下一步】按钮，打开如图 8-20 所示的【内容播放】对话框。在这里选择媒体文件内容连续播放的时候是循环播放还是无序播放，这可根据需要选择。



图 8-18 【发布点类型】对话框





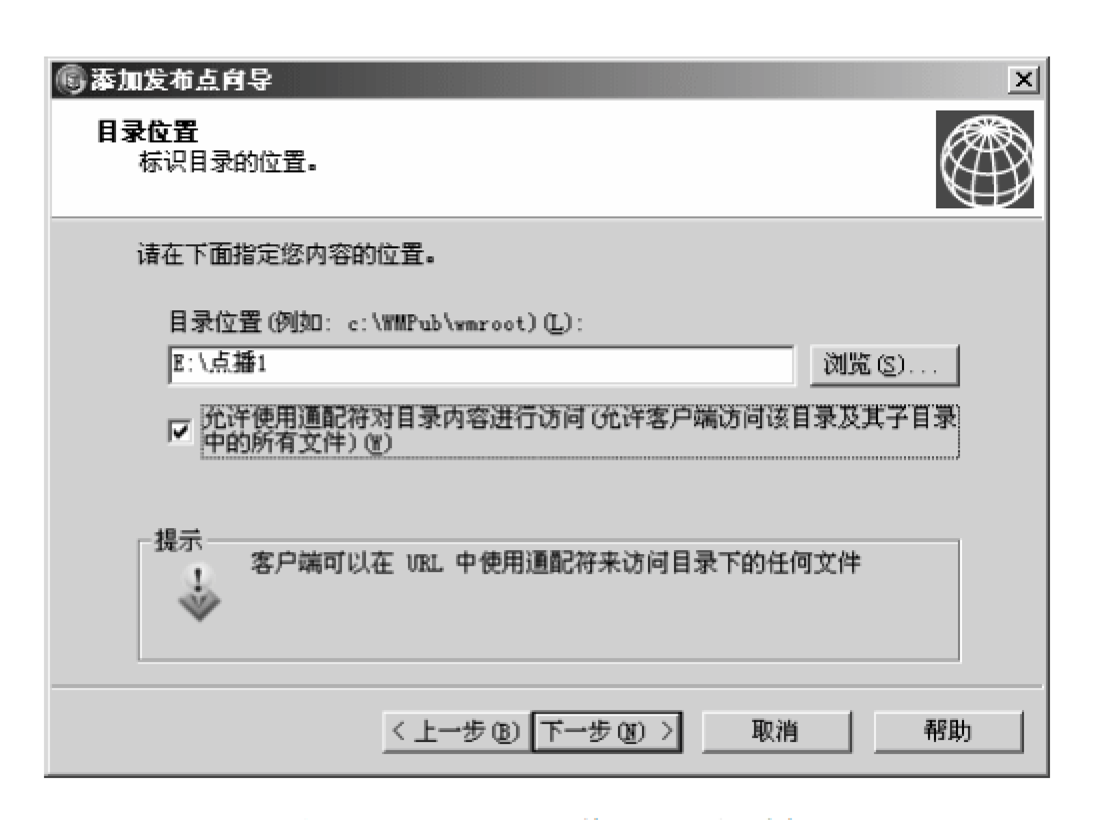


图 8-19　【目录位置】对话框

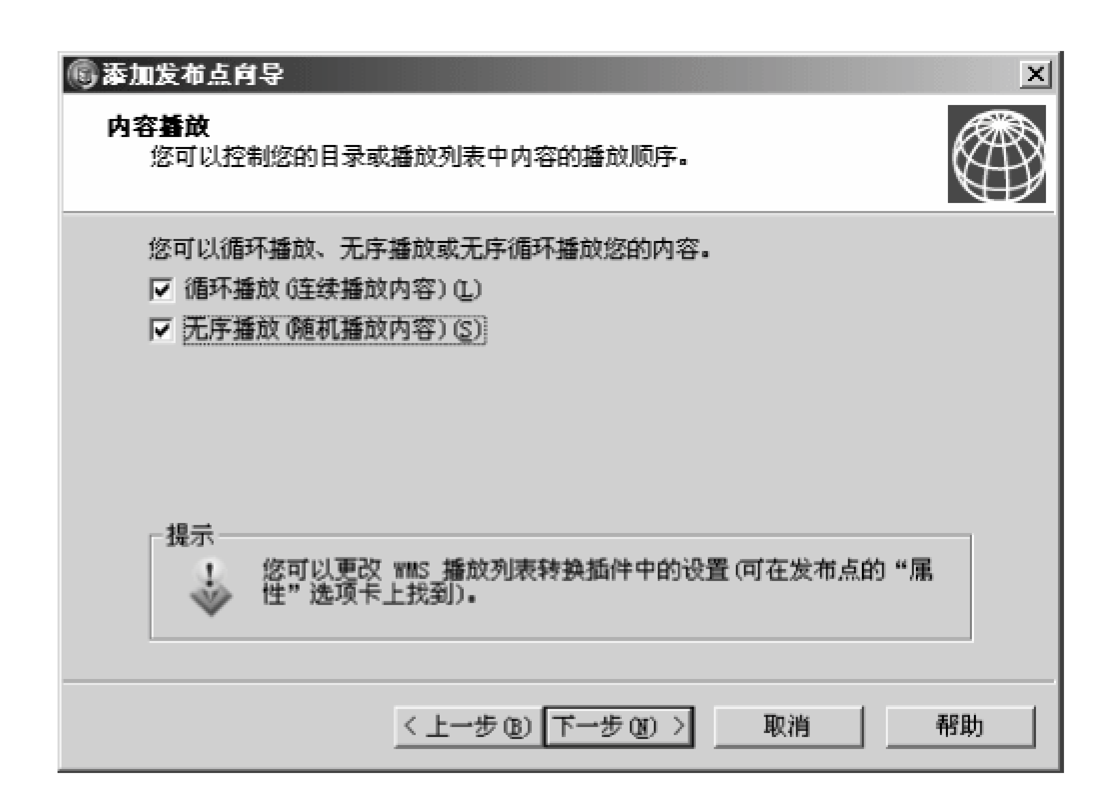


图 8-20　【内容播放】对话框

提示：循环播放：选择该复选框，可将发布点设成连续播放。对于点播发布点来说，在播放机停止流或者播放机断开之前，该流将重复播放。对于广播发布点来说，在服务器管理器停止流之前，该流将重复播放。

无序播放：选择该复选框，将发布点内容设成按随机顺序而不重复播放。

同时选择这两个复选框将为此发布点指定的内容提供连续、随机播放，并创建类似于无人参与的广播电台这样的用户使用效果。

(7) 单击【下一步】按钮，打开如图 8-21 所示的【单播日志记录】对话框，选择是否启用单播日志记录客户端的数据。

(8) 单击【下一步】按钮，打开如图 8-22 所示的【发布点摘要】对话框，以确认单播发布点相关设置是否正确。

(9) 核对配置后，单击【下一步】按钮，打开如图 8-23 所示的对话框。选中【完成向导后】复选框可以启动公告向导为这个发布点生成一个可供用户访问的包含媒体链接的网页。单击【完成】按钮，发布点即创建成功。

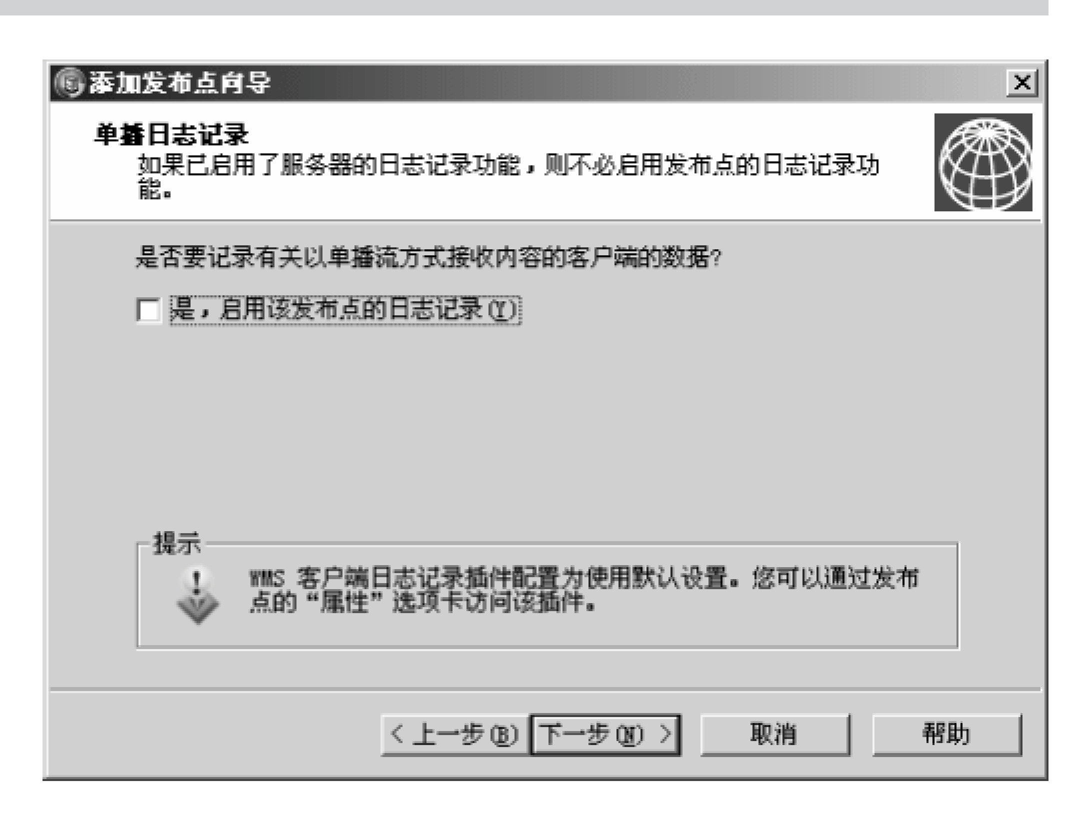


图 8-21　【单播日志记录】对话框

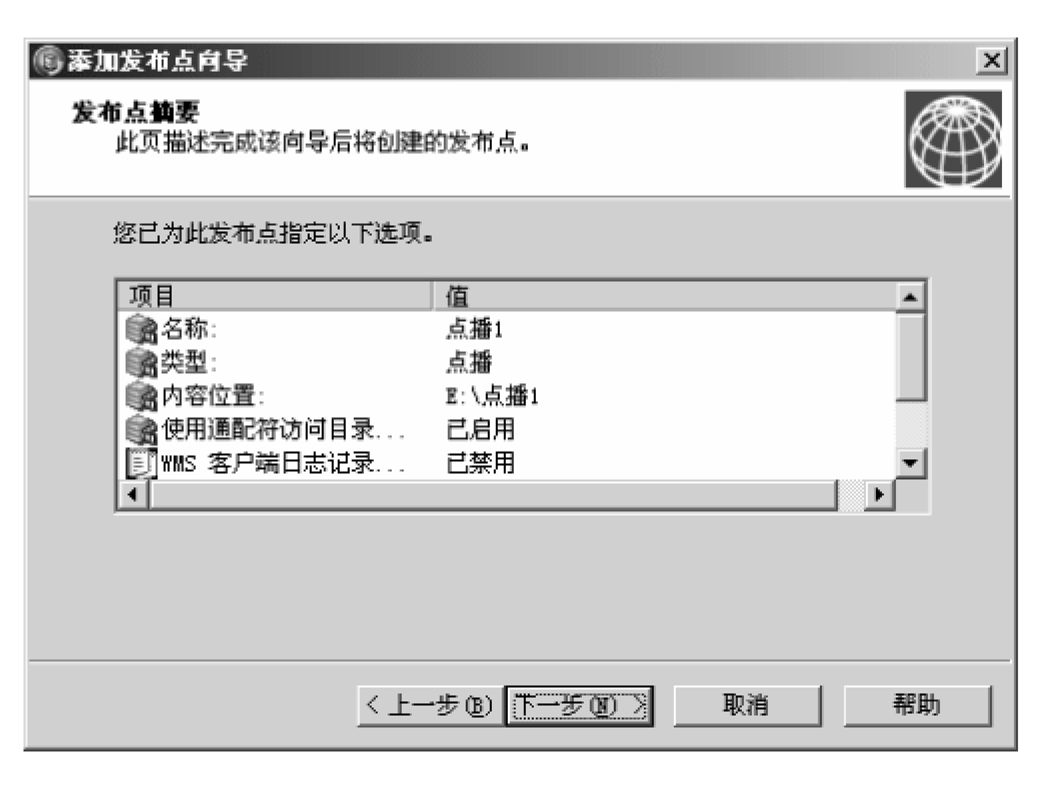


图 8-22　【发布点摘要】对话框



图 8-23　完成发布点添加





8.3.2 创建单播公告向导

在添加发布点完成后，进入如图 8-24 所示的【欢迎使用“单播公告向导”】对话框，继续按照以下步骤操作。

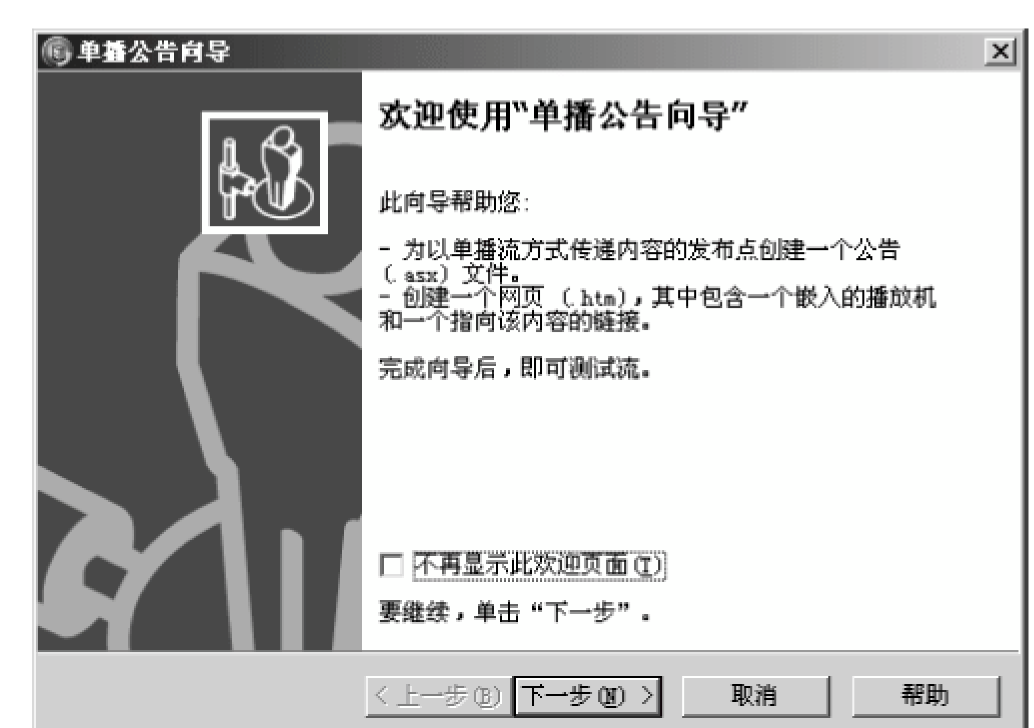


图 8-24 【欢迎使用“单播公告向导”】对话框

(1) 单击【下一步】按钮，打开如图 8-25 所示的【点播目录】对话框，选择公告的内容是一个文件还是目录中所有的文件。在此选择【目录中的所有文件】单选按钮。

(2) 单击【下一步】按钮，打开如图 8-26 所示的【访问该内容】对话框。本对话框中列出了访问当前内容的路径。

(3) 单击【下一步】按钮，打开【保存公告选项】对话框。选中【创建一个带有嵌入的播放机和指向该内容的链接的网页】复选框，然后单击【浏览】按钮，将公告文件名和创建的.htm 文件保存在发布点指定的目录中，如图 8-27 所示。



图 8-25 【点播目录】对话框



图 8-26 【访问该内容】对话框

(4) 单击【下一步】按钮，打开如图 8-28 所示的【编辑公告元数据】对话框。在这里可以输入标题、作者、版权等信息。

(5) 单击【下一步】按钮，出现如图 8-29 所示的【正在完成“单播公告向导”】对话框，选中【完成此向导后测试文件】复选框。

(6) 单击【完成】按钮，出现如图 8-30 所示的【测试单播公告】对话框。

(7) 单击【测试】按钮，便可在 Windows Media Player 或 Internet Explorer 的网页中播放，如图 8-31 和图 8-32 所示。

至此，单播公告创建完毕。管理员可以在网站上创建包含这些 URL 相应链接的网页来方便用户访问。用户也可以在浏览器或播放机(如 Windows Media Player)中用 URL “rtsp://主机地址/发布点名称/媒体文件名”或“mms://主机地址/发布点名称/媒体文件名”来访问发布点目录中的媒体文件，如图 8-33 所示。



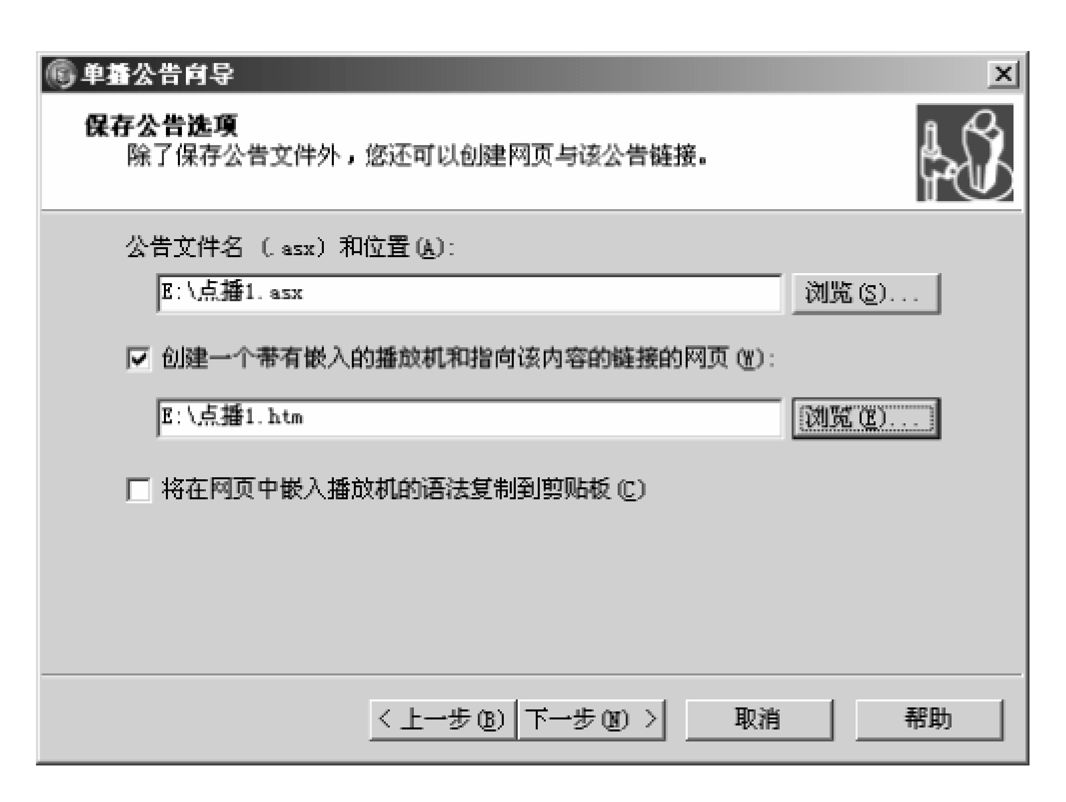


图 8-27　【保存公告选项】对话框



图 8-28　【编辑公告元数据】对话框



图 8-29　【正在完成"单播公告向导"】对话框

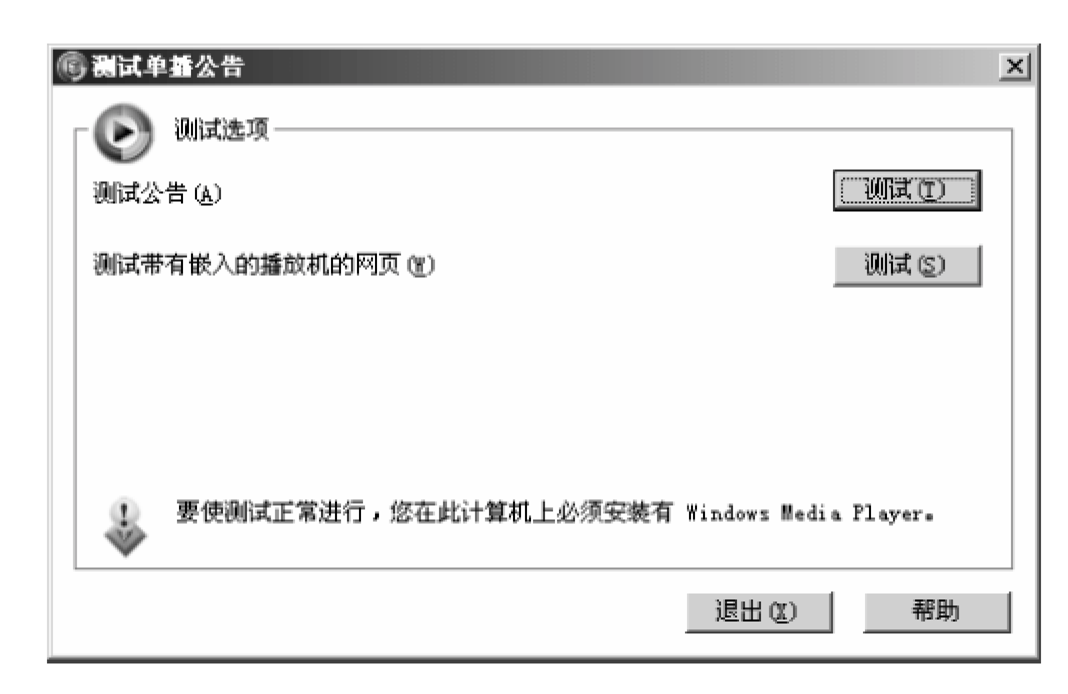


图 8-30　【测试单播公告】对话框



图 8-31　测试在 Windows Media Player 中播放





图 8-32　测试在 IE 中播放

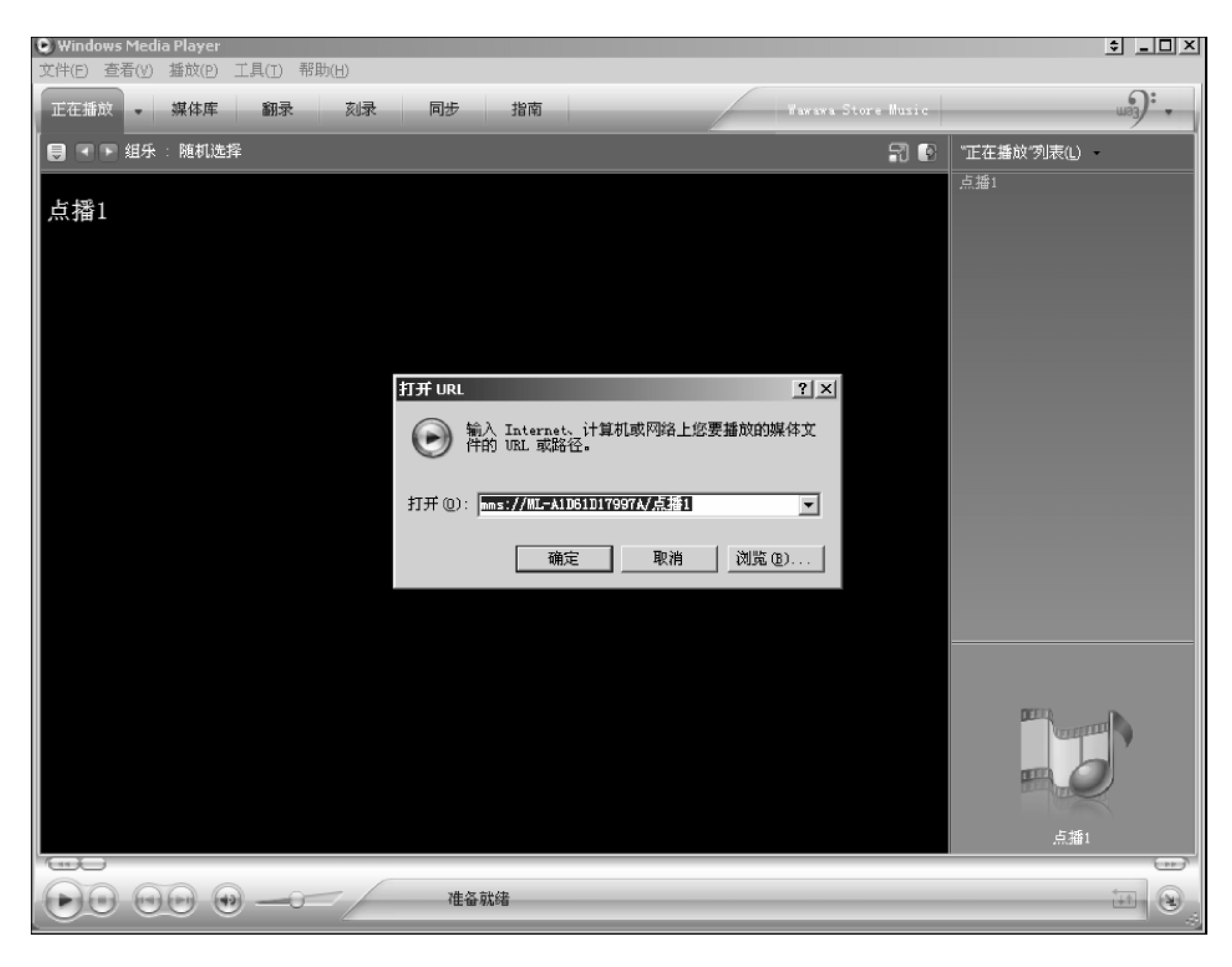


图 8-33　在 Windows Media Player 中播放发布点内容



技巧： 建立点播发布点有两种方法，即使用向导和高级方法。其中，在使用向导方法创建点播发布点时，用户只需在系统提示下设置各种参数即可。还可以自动生成ASX公告文件和HTML文件网页发布文件，以便于新手使用。而高级方法是指在一个Web页上完成各种参数的设置。实际上，高级方法其实更简单方便，但由于这种方法没有任何相关的提示，对用户的水平要求较高，所以不适合新手使用。如果是初次创建，建议先使用向导创建，待以后对各种参数和属性熟悉了以后，再用高级方法快速创建。

习　　题

1. 填空题

（1）与传统的多媒体下载不同，流媒体传输具有________和________的特点。

（2）流式传输是流媒体实现的关键技术，根据实现原理可分为________和________。

（3）一个最基本的流媒体系统包含________、________、________三个组件。

2. 选择题

（1）以下协议属与实时传输协议的是（　　）。

A. RTSP　　B. RTCP　　C. RTP　　D. RSVP

（2）以下播放器是Microsoft公司研发的是（　　）。

A. RealPlayer

B. Windows Media Player

C. Quicktime

D. Flash Player

3. 思考题

（1）何为流媒体？它的主要特点是什么？

（2）简述单播、组播、广播和点播。

4. 上机题

（1）安装Windows Media服务器。

（2）创建一个名为MV的发布点，发布点指向F盘的“播放”文件夹。



第9章　即时通信服务

本章要点

- 了解即时通信服务的基本概念及 Free ICQ 客户端和服务端有哪些主要功能
- 掌握如何安装并使用 FreeICQ 软件

即时通信(Instant Message,IM)是当今流行的一种以 Internet 网络及其他有线、无线网络为基础的实时通信方式。它通过通信系统建立网络虚拟社区,为用户提供实时有效的沟通手段。

9.1　即时通信服务概述

近年来,即时通信工具使用非常广泛,它已超出任何一种网络软件,成为最流行的互联网通信工具之一。

9.1.1　了解即时通信服务

即时通信是一个终端服务,允许两人或多人使用网络即时地传递文字信息、档案、语音与视频交流。它是一种使人们能在网上识别在线用户并与他们实时交换消息的技术,被称为电子邮件发明以来最酷的在线通信方式。

典型的 IM 是这样工作的:当好友列表中的某人在任何时候登录上线并试图通过你的计算机联系你时,IM 系统会发一个消息提醒你,然后你能与他建立一个聊天会话并输入消息文字进行交流。IM 被认为比电子邮件和聊天室更具有自发性,甚至你能在进行实时文本对话的同时一起进行 Web 冲浪。

目前常用的即时通信软件有腾讯 QQ、MSN、新浪 UC、雅虎通、TOM-Skype、移动飞信、FreeICQ 等。

9.1.2　了解即时通信软件——FreeICQ

很多人都习惯了用 QQ 进行交流,可有的单位的局域网并没有联上互联网。现在就介绍软件 FreeICQ,通过它,可以在局域网内组建一个即时通信服务器。

FreeICQ 是一套主要针对局域网的即时通信软件，包括服务器端和客户端。FreeICQ 采用类 OICQ 界面，操作简单快捷，而且对计算机的配置要求较低、安装简单，通过简单的设置就可以迅速地建立一个即时通信系统。

(1) FreeICQ 客户端的主要功能：

- 用户注册和登录；
- 接收/发送消息；
- 发送离线消息；
- 广播消息；
- 传送文件；
- 根据条件查找或查找在线用户，并将其加为好友；
- 声音和图标提示；
- 用户悬浮提示窗。

(2) FreeICQ 服务器端的主要功能：

- 用户管理；
- 日志管理；
- 查看在线用户；
- 系统广播消息；
- 编辑部门列表；
- 编辑链接地址。

9.2　安装 FreeICQ

FreeICQ 软件安装包包括服务器端安装文件和客户端安装文件。这里以最新版的 FreeServer0711.exe(服务器端)和 FreeICQ0904.exe(客户端)为例进行介绍。

9.2.1　FreeICQ 服务器端的安装

要想建立 FreeICQ 服务器，必须安装和配置好 TCP/IP 协议，并在服务器端安装有 Microsoft Access ODBC Driver(该程序在 Microsoft Office 系列中自带，一般在安装 Office 时选择完全安装)。

FreeICQ 服务器端的安装步骤如下：

(1) 双击下载的 FreeServer0711.exe 文件，进入 FreeICQ 服务器端安装向导，如图 9-1 所示。

(2) 单击【下一步】按钮，在出现的【许可协议】对话框中选中【我同意该许可协议的条款】单选按钮，如图 9-2 所示。

(3) 单击【下一步】按钮，出现安装目录设置对话框。这里选取默认设置，或者单击【更改】按钮，将程序安装到指定的位置，如图 9-3 所示。

(4) 单击【下一步】按钮，出现 FreeICQ Server 快捷方式设置对话框，如图 9-4 所示。



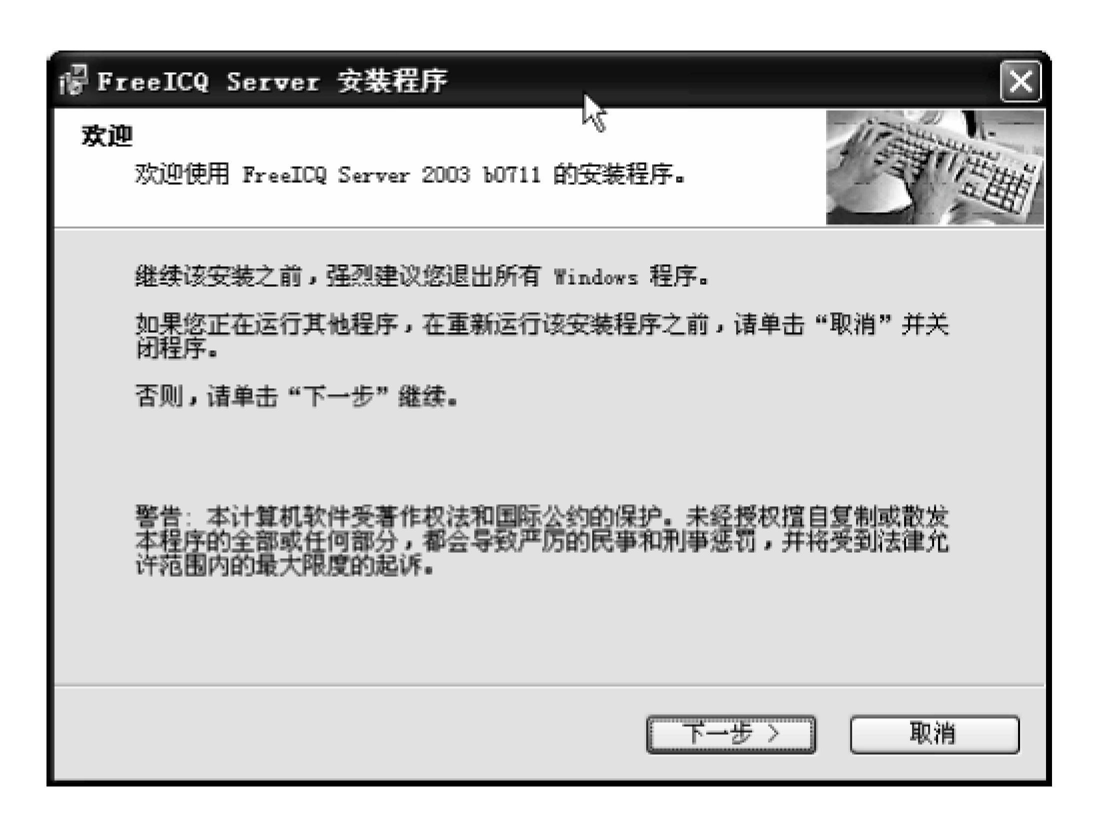


图 9-1　FreeICQ 服务器端安装向导



图 9-2　设置同意协议

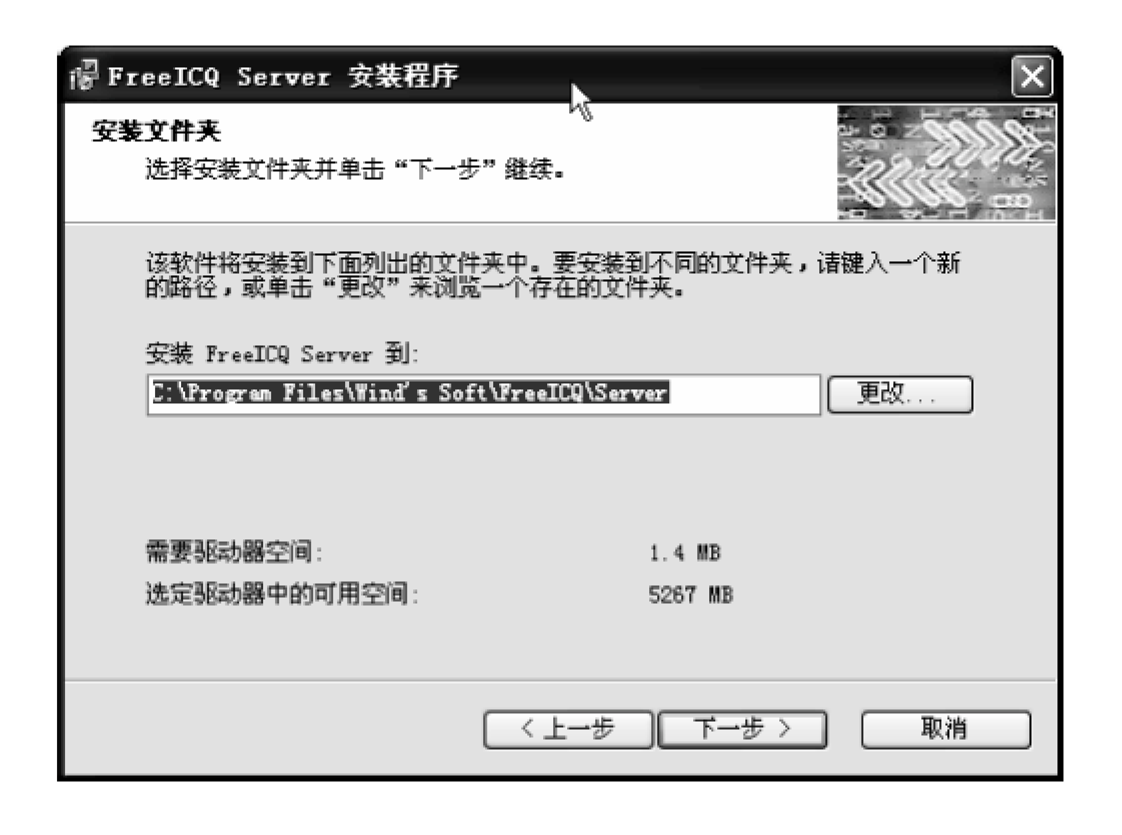


图 9-3　选取安装路径



图 9-4　设置服务器的快捷方式

（5）单击【下一步】按钮，出现安装前的准备对话框，如图 9-5 所示。

（6）单击【下一步】按钮，出现如图 9-6 所示的【安装完成】对话框。单击【完成】按钮，完成 FreeICQ 服务器端的安装。



图 9-5　安装前的准备对话框



图 9-6　服务器端安装完成



9.2.2　FreeICQ 客户端的安装

FreeICQ 客户端的安装步骤如下：

(1)双击下载的 FreeICQ0904.exe 文件，进入 FreeICQ 客户端安装向导，如图 9-7 所示。

(2) 单击【下一步】按钮，在出现的【许可协议】对话框中选中【我同意该许可协议的条款】单选按钮，如图 9-8 所示。

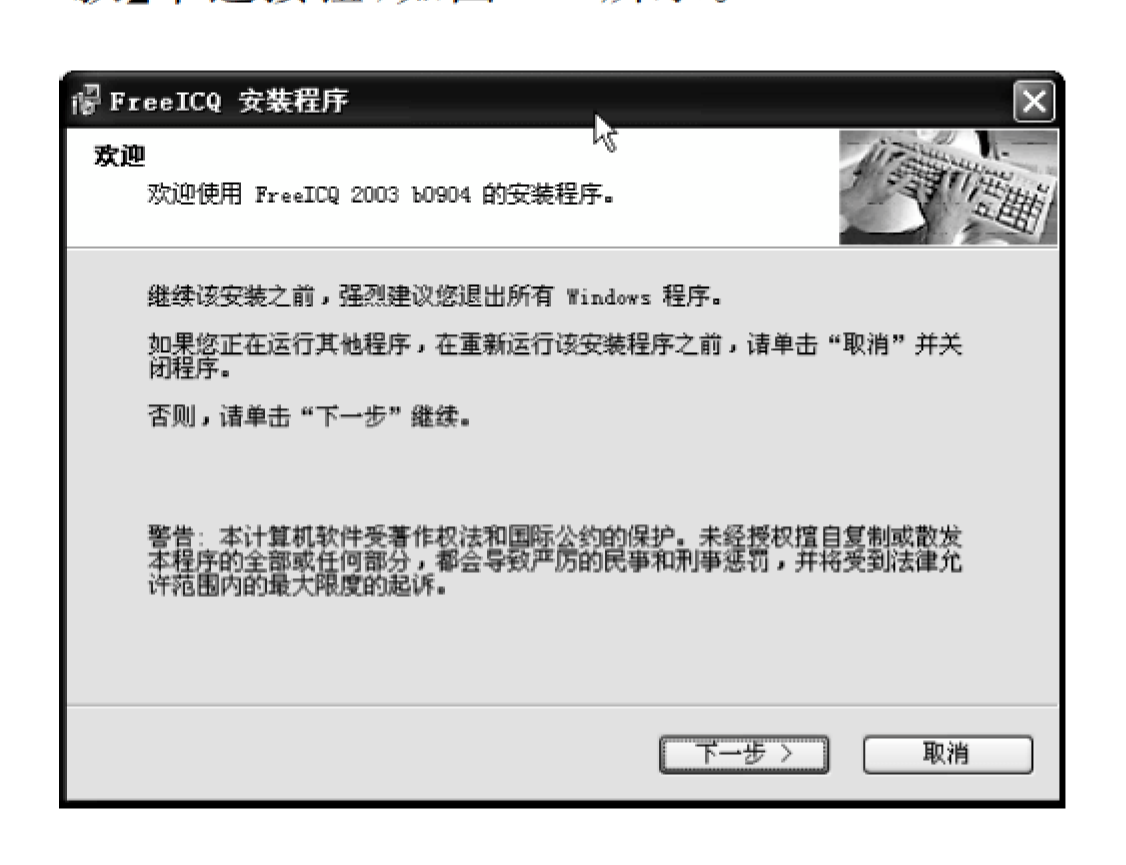


图 9-7　FreeICQ 客户端安装向导



图 9-8　设置同意协议

(3) 单击【下一步】按钮，出现安装目录设置对话框。这里选取默认设置，或者单击【更改】按钮，将程序安装到指定的位置，如图 9-9 所示。

(4) 单击【下一步】按钮，出现 FreeICQ 快捷方式设置对话框，如图 9-10 所示。

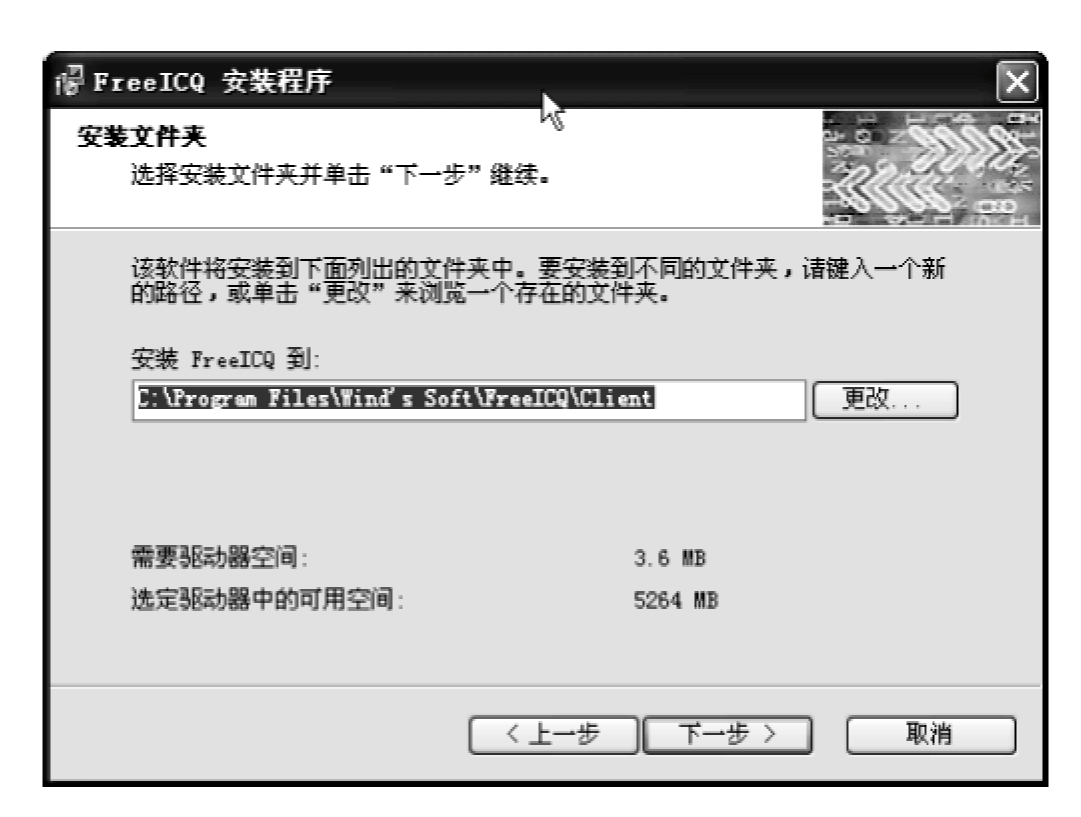


图 9-9　选取安装路径



图 9-10　设置客户端的快捷方式

(5) 单击【下一步】按钮，出现安装前的准备对话框，如图 9-11 所示。

(6) 单击【下一步】按钮，出现如图 9-12 所示的【安装完成】对话框。单击【完成】按钮，完成 FreeICQ 客户端的安装。







图 9-11　安装前的准备对话框



图 9-12　客户端安装完成

9.3　FreeICQ 服务器端的设置

服务器端安装结束后，依次选择【开始】→【程序】→FreeICQ Server→FreeServer 命令，打开 FreeICQ 服务器软件，出现如图 9-13 所示的 FreeICQ Server 窗口。在打开的窗口中单击【管理工具】按钮就可以开始配置服务器了。



图 9-13　FreeICQ Server 窗口

提示：FreeICQ Server 窗口为服务器程序的主窗口，在提供即时通信服务或利用管理工具进行配置时，要始终打开此窗口，不要将其关闭。

FreeICQ Server 的管理工具中共有六个选项卡，下面依次进行介绍，并对 FreeICQ 服务器进行配置。

1.【控制】选项卡（如图 9-14 所示）

- 【开始】和【停止】按钮。控制 FICQ 服务器（即 FreeICQ Server）的启动和停止。
- 【刷新在线列表】按钮。查看局域网内的即时在线网友，包括号码、昵称、IP、部门等。

2.【用户管理】选项卡（如图 9-15 所示）

可以查看、增加、删除已经申请 FICQ 号的网友的各种个人信息。





图 9-14　FreeICQ 管理【控制】选项卡



图 9-15　【用户管理】选项卡

（1）查询用户。选中【所有用户】单选按钮，选择一种合适的排序方式（如按 FICQ 号、部门、IP 地址、性别等排序，默认情况下程序会按 FICQ 号大小来排序），单击【执行查询】按钮，则所有已注册的用户记录就会自动显示在【查询结果】列表中。

（2）添加用户。单击【新增】按钮，出现【用户资料】对话框，如图 9-16 所示。添加完用户资料后，单击【确定】按钮即可完成增加新用户。

（3）删除用户。选中一个查询结果，单击【删除】按钮，可以删除相应用户。

（4）查看/修改用户属性。

- 单击【查看/修改属性】按钮，可以更改用户的个人信息，如用户名、密码等。
- 设置客户端用户的广播权限。在用户资料的【其他设置】选项卡中设置好对应该用户的广播权限。



图 9-16　【用户资料】对话框

3．【安全】选项卡（如图 9-17 所示）

可以禁止一些 IP 地址访问服务器。单击【添加】、【删除】或【修改】按钮可以对禁止访问的 IP 地址进行相应操作。

4．【日志】选项卡（如图 9-18 所示）

可以查看用户使用 FICQ 的情况，如用户的号码是在什么时候申请到的、用户是在什么时间登录进服务器中的、用户是在什么时候离线的等。

5．【服务端消息】选项卡（如图 9-19 所示）

- 向所有用户广播服务器消息。把广播信息输入到文本框中，选择好【广播类型】和



【广播范围】，单击【广播】按钮。

• 【服务器消息】列表中的内容，就是指所有具有广播权限的网友在 FICQ 客户端广播的消息，可以进行刷新、查看、删除等操作。



图 9-17 【安全】选项卡



图 9-18 【日志】选项卡

6.【设置】选项卡(如图 9-20 所示)

• 单击【设置/修改管理员密码】按钮，在随后打开的窗口中设置好一个口令，这样可以防止不法用户登录到 FICQ 服务器中。这是因为 FICQ 服务器端既可以运行在 Windows 2000 系统上，还能运行在 Windows 9x 系统上，因此设置合适的登录密码是非常有必要的。

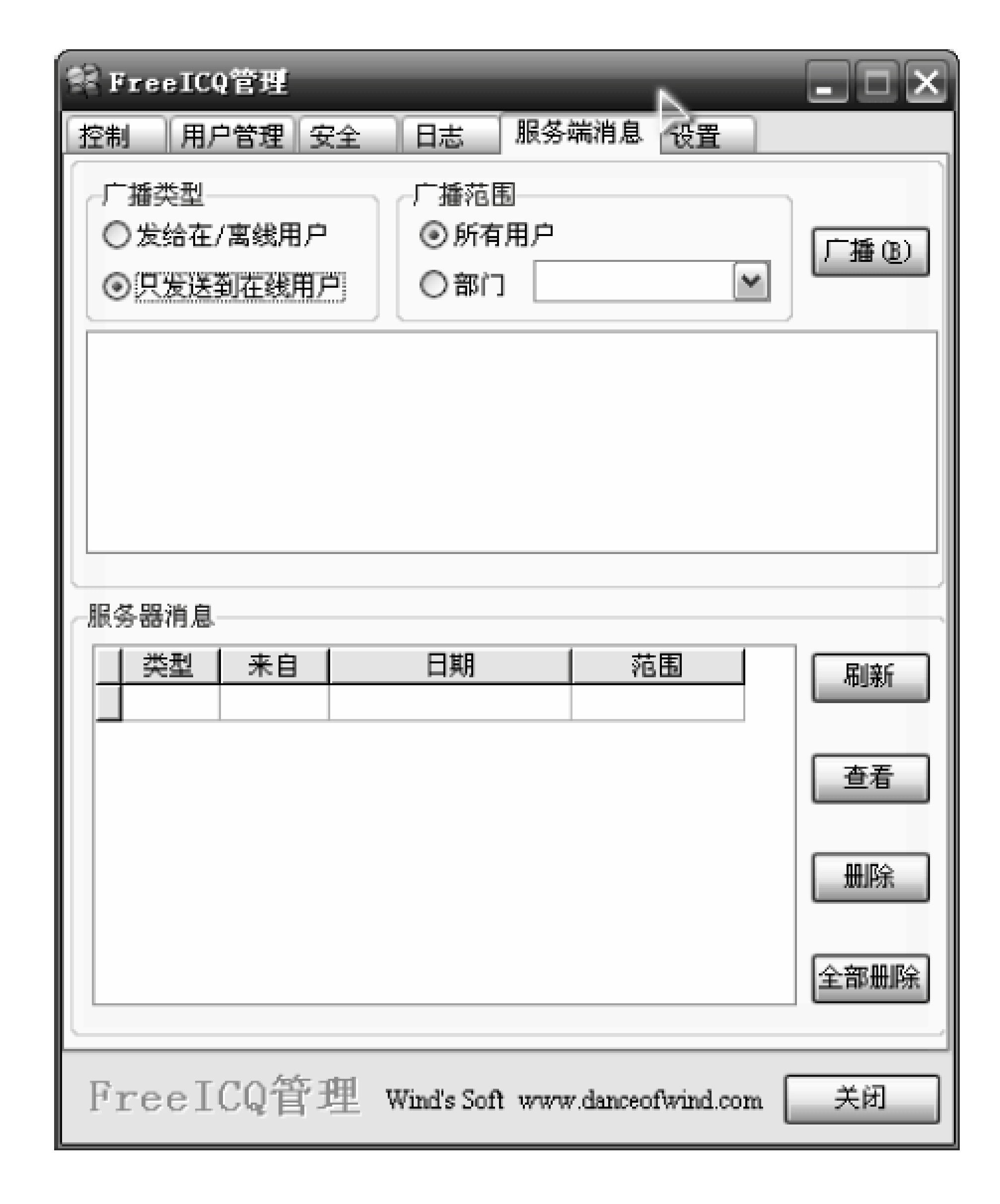


图 9-19 【服务端消息】选项卡



图 9-20 【设置】选项卡



- 单击【编辑/更新部门列表】按钮，就能自定义部门参数了。根据局域网内部的使用情况，该部门选项在广播消息时，既能单独广播到一个部门，也能广播到所有部门。

9.4　FreeICQ 客户端的设置

FreeICQ 客户端软件的使用也相当简单，下面简单介绍一下其基本的使用和设置。

9.4.1　用户注册和登录

客户端安装完毕，依次选择【开始】→【程序】→FreeICQ→FreeICQ 命令，打开 FreeICQ 客户软件，任务栏中将显示其图标（该图标随在线状态改变），同时打开图 9-21 所示的【FICQ 用户登录】对话框。

1．注册新用户

初次使用时需要注册新的用户账号，具体的操作步骤如下：

（1）单击【注册向导】按钮，打开图 9-22 所示的【选择注册方式】对话框。这里选中【注册新的 FICQ 号码】单选按钮（如果选中【使用已有的号码】单选按钮，可以将以前申请的账号信息加入到本地 FreeICQ 客户）。单击【下一步】按钮。




图 9-21　【FICQ 用户登录】对话框



图 9-22　【选择注册方式】对话框

（2）打开图 9-23 所示的【网络设置】对话框。在【服务器地址】文本框中输入 FreeICQ 服务器的 IP 地址，【端口号】保持默认值。如果通过代理服务器来访问 FreeICQ 服务器，应选中【使用 Socks5 代理】复选框，在【防火墙地址】文本框中输入代理服务器地址，并设置其他选项。

（3）单击【下一步】按钮，接下来的两步是设置用户的基本资料和详细资料，分别如图 9-24 和图 9-25 所示。除了昵称和密码必须输入外，其他项都是可选输入项。

（4）最后出现注册成功的对话框，并给出注册的号码，如图 9-26 所示。单击【完成】按钮完成新用户注册。





图 9-23 【网络设置】对话框



图 9-24 基本资料



图 9-25 详细资料



图 9-26 注册完成

2. 用户登录

新用户注册完成后，申请了一个号码为 1001 的用户，用户昵称为“小明”。

同样，也可以申请一个号码为 1002 的用户，用户昵称为“小张”。

两个用户分别登录，在图 9-27 所示对话框中分别输入小明、小张的 FreeICQ 号码和密码，单击【登录】按钮就可以登录进入 FreeICQ 客户端主界面，如图 9-28 所示。



(a) 小明的登录界面



(b) 小张的登录界面

图 9-27 【FICQ 用户登录】对话框

小明和小张相互加对方为好友，便可在自己的好友列表中看到对方，如图 9-29 所示。

两个用户之间可以相互发送消息、聊天、收发文件或者下象棋等，如图 9-30 所示。







(a) 小明的号码




(b) 小张的号码

图 9-28　FICQ 用户端主界面



(a) 小明的好友



(b) 小张的好友

图 9-29　相互加为好友后的界面



图 9-30　FICQ 聊天记录

9.4.2　客户端设置

可通过客户端设置来修改用户资料。右击任务栏中的 FICQ 客户图标，打开图 9-31 所示的 FICQ 客户设置快捷菜单。选择【个人设定】命令，打开【用户资料】窗口。除了修改个人的基本信息之外，还可切换到如图 9-32 所示的【网络安全】选项卡，从中修改用户密码或选择身份验证方式。

在 FICQ 客户设置快捷菜单里选择【系统设置】命令，打开图 9-33 所示的【系统设置】对话框其中的【参数设置】选项卡用来设置客户端基本参数。

技巧： 利用 FICQ 客户设置快捷菜单，可以对自己的 FICQ 客户端进行个性化设置，使其在使用中更符合自己的习惯和要求。例如，如果想在使用 FICQ 时不被别人打扰，可以设置以隐身方式登录等。





图 9-31　FICQ 客户设置快捷菜单



图 9-32　【网络安全】选项卡

9.4.3　FreeICQ 的基本使用

最后讲述 FreeICQ 的基本使用步骤。首先要查找在线用户，可输入对方的号码、昵称或部门，来查找当前在线用户，将其加入为好友。然后从【我的好友】列表中单击某个用户，从弹出的如图 9-34 所示的 FreeICQ 功能选择菜单中选择所需的功能。例如，收发消息、传送文件，还可以进行语音聊天、下中国象棋等。



图 9-33　【参数设置】选项卡



图 9-34　FreeICQ 功能选择菜单

9.5　疑难解答

(1) 一般在什么情况下安装使用 FreeICQ?

FreeICQ 是多种即时通信软件中的一种，主要针对局域网的用户使用，包括服务器端和客户端。FreeICQ 软件功能没有腾讯公司的 QQ 强大，但它解决了没有连接互联网的内部



局域网用户的需要。操作简单快捷,对计算机的配置要求较低、安装简单,通过简单的设置就可以在局域网内迅速地建立一个即时通信系统。

(2) 如何对 FreeICQ 服务器端进行配置?

服务器端安装结束后,在打开的主程序窗口中单击【管理工具】按钮就可以开始配置服务器了。对服务器端进行配置的过程,其实就是对 FreeICQ 服务器端进行管理和使用的过程,共分控制、用户管理、安全、日志、服务端消息和设置六个选项卡。在对服务器进行配置时,只需根据实际情况和服务需要,对这六项内容逐一进行设置即可。

(3) 使用客户端注册新用户时无法完成注册是什么原因?

一是服务器或代理服务器地址没有填写正确,要输入正确的 FreeICQ 服务器端(安装了 FreeICQ Server 的计算机)的 IP 地址,【端口号】保持默认值。如果是通过代理服务器来访问 FreeICQ 服务器,应选中【使用 Socks5 代理】复选框,在【防火墙地址】文本框中输入正确的代理服务器地址,并设置其他选项;二是用户资料没有输入完整,设置用户的基本资料和详细资料,除了昵称和密码必须输入外,其他项都是可选输入项。

(4) 使用客户端如何实现对多个用户同时发送消息?

可以使用群发信息的功能。群发信息可以同时将一个新信息发送给一个或多个在线好友。先双击任意一个在线好友名以打开发送信息的窗口。写好正文后,再单击窗口右上方,即头像下面的【>>】按钮。此时右侧会多连出一个小窗口,其中显示的是你的所有在线和不在线的好友。选中所需要的名字,最后单击【发送信息】按钮即可成功完成群发操作。

习　　题

1. 填空题

(1) FreeICQ 是一套主要针对局域网的即时通信软件,包括________和________。

(2) FreeICQ Server 的管理工具中共有六个选项卡,分别是控制、________、安全、________、服务端消息和________。

2. 选择题

(1) 目前常用的即时通信软件有(　　)。

A. 腾讯 QQ　　B. MSN　　C. FreeICQ　　D. 迅雷

(2) FreeICQ Server 的管理工具中【用户管理】选项卡可以进行的设置包括(　　)。

A. 查询用户　　B. 添加用户

C. 删除用户　　D. 查看/修改用户属性

3. 思考题

(1) 什么是即时通信?提供即时通信服务的软件都有哪些?

(2) 如何对 FreeICQ 服务器端进行设置?

4. 上机题

(1) 对 FreeICQ 服务器设置管理员密码。

(2) 使用 FreeICQ 查找在线用户,将其加入为好友,并收发消息、传送文件。

第10章　索引服务

本章要点

- 搜索引擎概述
- 微软索引服务介绍
- 索引服务的管理
- 建立和维护索引
- 使用索引查询

索引服务(Indexing Service)是 Windows Server 2003 系统中的一项基础服务,它可以使本地文件系统和本地 Web 服务器中的文档及文档信息管理、查询起来更高效、更快速。索引服务可对本地磁盘上的文档和文档属性进行索引处理,并将相关信息存储在目录中,从而通过 Windows 搜索功能、索引服务查询表或 Web 浏览器快速容易地访问某一指定的信息。该信息可以包含文档的内容、文档的特征和参数(属性)。索引服务也包含在 Internet 信息服务器(IIS)中,可使用编程语言对其进行访问和调用,从而能够建立本地站点的搜索引擎,检索本地资源。

10.1　搜索引擎概述

传统的索引是指一种排序技术,它不改变数据表中数据的物理顺序,只是另外建立一个记录列表,与常见的图书目录相似。所不同的是,图书中的目录指明的是章、节、页码,记录列表的索引指明的是由某一字段的值的大小决定的记录排列的顺序。

搜索引擎(Search Engine)是指一种能够提供检索服务的技术和系统。该系统根据一定的策略、运用特定的程序搜集互联网上的信息,然后对信息进行组织和处理,最后为用户提供各种相关的检索结果。搜索引擎提供一个包含搜索框的交互页面,用户在搜索框中输入关键词后,该搜索便通过浏览器提交给查询机制,查询机制返回与输入内容相关的信息列表。该技术和系统最初是用来查找散布于网络中各主机上的文件。随着互联网的出现和应用及其相关技术的迅速发展和普及,全球电子信息急剧增长,为满足大众信息检索需求的搜索引擎便应运而生。现在,搜索引擎成了互联网上可以查询网站或网页信息的主要工具。



10.1.1　搜索引擎的发展

最早的搜索引擎是1990年由加拿大麦吉尔大学学生Alan Emtage、Peter Deutsch、Bill Wheelan发明的Archie(Archie FAQ)。当时互联网(Internet)还未出现，网络的主要用途是传输文件。由于大量的文件散布在各个分散的FTP主机中，查询起来非常不便，Alan Emtage开发了一个可以以文件名查找文件的系统——Archie。

1993年，Gopher出现。在万维网(World Wide Web，WWW)出现之前，Gopher软件是互联网(Internet)上最主要的信息检索工具，Gopher站点也是最主要的站点。当万维网出现后，Gopher逐渐失去其昔日的地位，但因Gopher站点能够容纳大量的信息，可供用户查询，直到今天仍在使用。

1994年1月，第一个既可搜索又可浏览的分类目录TradeWave Galaxy(原名为EINet Galaxy，由TradeWave公司编制)出现。除了网站搜索，它还支持Gopher和Telnet搜索。

1994年4月，斯坦福(Stanford)大学的两名博士生，David Filo和美籍华人杨致远(Jerry Yang)共同创办了超级目录索引——Yahoo，从此搜索引擎进入了高速发展时期。

1995年12月，DEC公司(Digital Equipment Corporation)的AltaVista登场，大量的创新功能使它迅速到达当时搜索引擎的顶峰。AltaVista是第一个支持自然语言搜索的搜索引擎，AltaVista是第一个实现高级搜索语法的搜索引擎。

1998年9月，Google诞生。Google的前身是Stanford大学的一个小项目BackRub。1995年博士生Larry Page开始学习搜索引擎设计，于1997年9月15日注册了google.com的域名。1997年年底，在Sergey Brin和Scott Hassan、Alan Steremberg的共同参与下，BachRub开始提供Demo。1999年2月，Google完成了从Alpha版到Beta版的升级。Google以网页级别为基础，判断网页的重要性，使得搜索结果的相关性大大增强。通过对20多亿网页进行整理，Google可为世界各地的用户提供适需的搜索结果。

北大天网是国家“九五”重点科技攻关项目“中文编码和分布式中英文信息发现”的研究成果，由北大计算机系网络与分布式系统研究室开发，于1997年10月29日正式在CERNet上提供服务。

2000年1月，两位北大校友，前Infoseek资深工程师李彦宏与加州大学伯克利分校博士后徐勇在北京中关村创立了百度(Baidu)公司。2001年8月发布Baidu.com搜索引擎Beta版，2001年10月22日正式发布Baidu搜索引擎，专注于中文搜索。Baidu搜索引擎的其他特色包括百度快照、网页预览、相关搜索词、错别字纠正提示、mp3搜索、Flash搜索。2002年3月闪电计划(Blitzen Project)开始后，技术升级加快。之后推出贴吧、知道、地图、国学、百科、文档、博客、视频等一系列产品。

1996年8月，Sohu公司成立，专注于制作中文网站分类目录，随着互联网网站的急剧增加，这种人工编辑的分类目录已经不适应。Sohu公司于2004年8月推出独立域名的搜索网站“搜狗”，自称“第三代搜索引擎”。

2005年6月，新浪正式推出自主研发的搜索引擎“爱问”。2007年起，新浪爱问使用Google搜索引擎。



10.1.2 搜索引擎的原理

搜索引擎是目前互联网对信息资源进行组织的主要方式。大致可以分为三步：从互联网上抓取网页；建立索引数据库；在索引数据库中搜索并对结果排序。

(1) 抓取网页。利用能够从互联网上自动收集网页的网上机器人程序(Spider 或 Robot)自动访问互联网。Spider 或 Robot 是一种软件，它沿着互联网上的文件链接在网上漫游，记录 URL、文件的简明摘要、关键字或索引，形成一个大数据库。这个数据库包括标题、摘要、关键词和 URL、文件的大小、语种以及词出现的频率，并沿着任何网页中的所有 URL 爬到其他网页，重复这一过程，并把爬过的所有网页收集回来。

(2) 建立索引数据库。索引分析程序对收集回来的网页进行分析，提取相关网页信息，包括网页所在 URL、编码类型、页面内容包含的关键词、关键词位置、生成时间、大小、与其他网页的链接关系等，根据一定的相关度算法进行计算，得到每一个网页针对页面内容中及超级链接中每一个关键词的相关度，然后用这些相关信息建立网页索引数据库。

(3) 在索引数据库中搜索并对搜索结果排序。输入关键词搜索后，搜索程序从网页索引数据库中找到符合该关键词的所有相关网页，计算出所有相关网页针对该关键词的相关度，以相关度数值排序，相关度越高，排名越靠前。最后，由页面生成系统将搜索结果的链接地址和页面内容摘要等内容组织起来返回给用户。

10.1.3 搜索引擎的组成

搜索引擎一般由搜索器、索引器、检索器和用户接口这四部分组成。

搜索器的功能是在互联网中漫游，发现和搜集信息。

索引器的功能是理解搜索器所搜索到的信息，从中抽取出索引项，用于表示文档以及生成文档库的索引表。

检索器用来在索引库中快速检索用户查询的文档，并进行相关度评价，对要输出的结果排序，并能按用户的查询需求合理反馈信息。

用户接口是为用户提供查询、显示查询结果、提供个性化查询项的用户操作界面。

10.1.4 搜索引擎的分类

搜索引擎按其工作方式主要可分为三种：全文搜索引擎(Full Text Search Engine)、目录索引类搜索引擎(Search Index/Directory)、元搜索引擎(Meta Search Engine)。

(1) 全文搜索引擎。全文搜索引擎是最常用的搜索引擎，通过从互联网上提取的各个网站的信息而建立的数据库中，检索与用户查询条件匹配的相关记录，然后按一定的排列顺序将结果返回给用户。

(2) 目录索引类搜索引擎。目录索引类搜索引擎虽然有搜索功能，但严格意义上不能



称为真正的搜索引擎,只是按目录分类的网站链接列表。用户可以按照分类目录找到所需要的信息,不依靠关键词(keywords)进行查询。与全文搜索引擎的区别在于它是由人工建立的,通过"人工方式"将站点进行了分类,不像全文搜索引擎那样,将网站上的所有文章和信息都收录进去,而是首先将该网站划分到某个分类下,再记录一些摘要信息。

(3) 元搜索引擎。元搜索引擎接受用户查询请求后,同时在多个搜索引擎上搜索,并将结果返回给用户。著名的元搜索引擎有 InfoSpace、Dogpile、Vivisimo 等,中文元搜索引擎中具代表性的有搜乐搜索(www.sooule.com)、万维搜索(www.widewaysearch.com)等。在搜索结果排列方面,有的直接按来源排列搜索结果,如 Dogpile;有的则按自定的规则将结果重新排列组合,如 Vivisimo 等。

10.2　微软索引服务

微软索引服务(Microsoft Indexing Service)由系统自带的微软索引服务器(Index Server)提供,索引服务器集成于 Internet 信息服务器(IIS) 6.0 和 Windows Server 2003 操作系统中。索引服务可以把网络搜索功能引入到 Web 网站中,建立一个本地的网络服务器索引,使用户通过相同的查询表格就可从 Web 浏览器中进行搜索操作。

10.2.1　微软索引服务的来历

最早,微软为更好地解决网站搜索功能而开发了索引服务,索引服务的核心来自于目录索引器(Content Indexer)。目录索引器是 Windows NT 系统的基础技术之一,它被设计成比传统搜索方案更具可靠性、持续性和有效性的索引技术。索引服务是在目录索引器的基础上,为 Web 应用而开发的索引技术。1996 年 8 月,索引服务器的第一个版本发行,在 1996 年 12 月该版本又做了增改。直到 1997 年 10 月,Index Server 1.0 和 Index Server 1.1 一直为 Microsoft Windows NT Server 4.0 和 Internet 信息服务器(IIS) 3.0 服务。后来,Index Server 2.0 在 Windows NT Server 4.0 的选项包中发布,且只安装在 Web 服务器上,普通机器没有安装。Index Server 2.0 支持 ASP 编程,支持更多的检索文件类型,支持多种语言,维护量更少。在 Windows Server 2000 之后的所有版本中,系统都带有 Index Server 3.0。在默认情况下,Index Server 3.0 都已安装但并不运行。

10.2.2　微软索引服务的工作原理

索引服务将其所有的索引信息存储在编录中。编录中包含了文档和文件夹的索引信息和存储属性。Windows Server 2003 安装索引服务后,将自动构造系统编录(System 编录)和 Web 编录,前者列出了所有永久连接磁盘驱动器的内容,后者则包含 Internet 信息服务器(IIS)相关目录内容。

索引服务器不会按正常方式来检查被修改的文档,这样做会加重系统资源的负担。索引服务器的工作方式是在文件系统中登记,以得到文件被改变的通知信息,并且仅在合适的时候更新索引。当一个 NTFS 卷标中的文档被修改后,文件系统将通知索引服务器。索引



服务器并不马上索引该文档，索引将在后台进行，并且仅在有足够的计算机资源时发生，这样就不会影响整个系统的性能。当索引服务器确定它可以索引发生的变化后，它将打开变化的文档，然后开始索引过程。

索引服务的实现包括索引过程和查询过程。

1. 索引过程

索引过程对索引文件进行预处理，形成编录文件，使查询工作得以进行。索引过程通常在索引服务初始化时进行。这一过程就像图书馆的编目工作，在书库的成千上万本书中找到想要的一两本书不是件容易的事情。需要先对所有的图书进行编目，形成分类目录、书名目录和作者目录，依赖于这些目录的索引，才能快速准确地找到目标。相应的，索引服务也需要对目录文件进行预处理，也就是索引过程。查询功能其实是在索引过程形成的编录文件中进行查询工作。

索引过程的工作原理如图 10-1 所示。

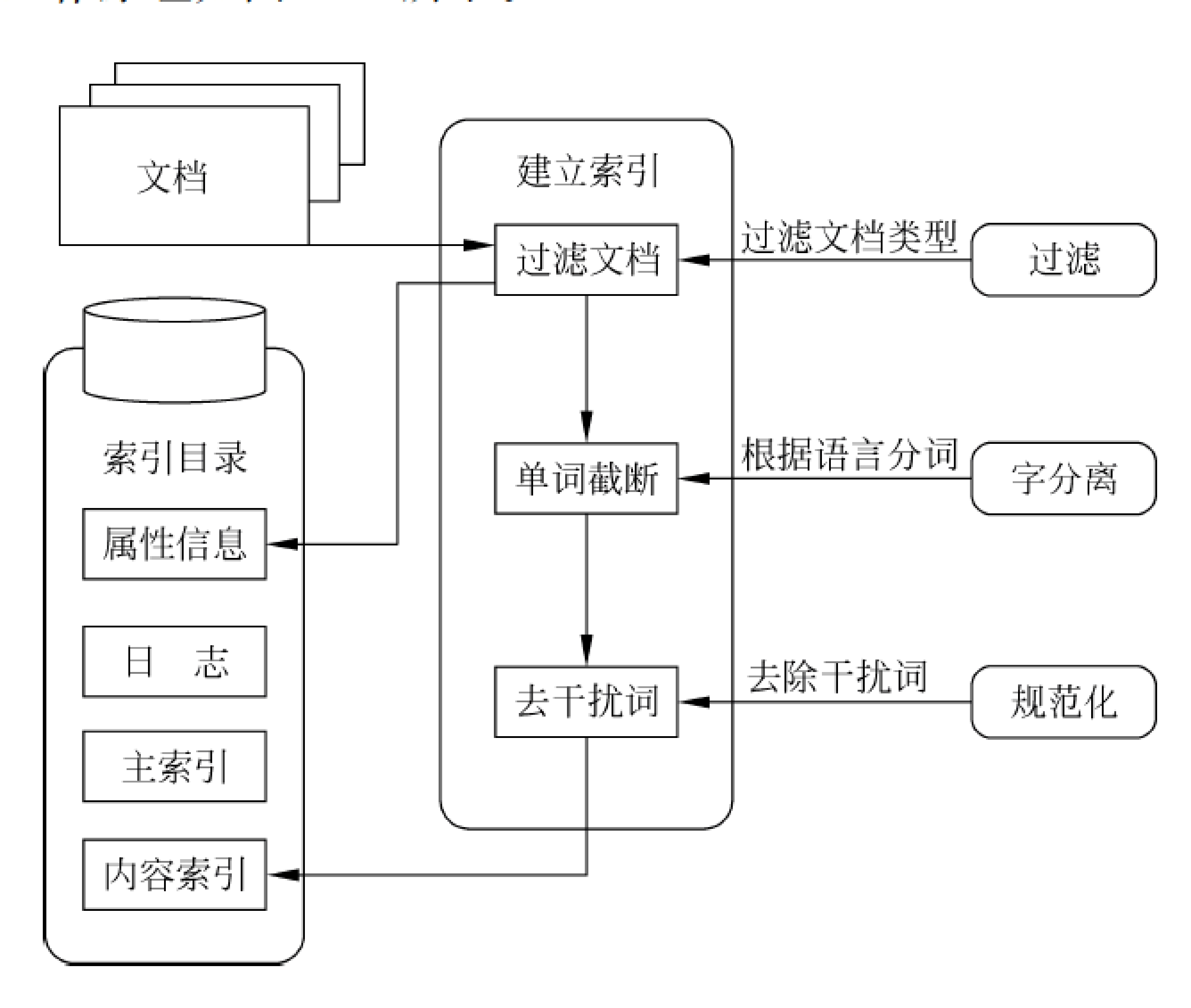


图 10-1　索引过程的工作原理

索引过程大体上包括三个步骤：过滤、字分离和规范化。

（1）过滤(Filter)。索引的第一个步骤是内容过滤。文档一般都是以特定的文件格式存储，这些格式对系统是不透明的，许多内容索引系统不能读取这些文件格式，所以系统不能对这些文件进行索引。索引服务器使用了开放式标准的内容过滤器来索引特定的文件格式，一个内容过滤器可以看作是一个应用程序的小型版本，其功能是对这个应用程序自身文件进行读取。

当索引服务器开始对一个文档进行操作时，它将确定文档的类型，并使用合适的内容过滤器。过滤器从文档中提取出文本的主干，然后以索引服务器可以识别的格式传送到系统中。除了提取文本主干外，内容过滤器的另一个重要功能是识别文档中所使用语言的转换。有些文档格式将指示文本某一部分所使用的语言，如果这些标签存在，内容过滤器将根据这





些标签对某一部分的文本进行对应的操作。内容过滤器也负责处理嵌入对象，当在一个文档中出现嵌入对象时，它的类型将被识别，并且相应的过滤器将激活。这表示索引服务器不仅能够索引一个 Word 文档中的文本，也能够索引嵌入到该 Word 文档中的 Excel 电子表格中的任何文本。

(2) 字分离(Word Break)。在过滤后，下一个任务是字分离。数据经过过滤器后成为字符流，由索引服务器对字进行索引。不同的语言以不同的方式处理字，以不同方法分离字。索引服务器提供了针对不同语言的字分离器，这些分离器知道如何分离字符流成为有效的字。这些模块能够理解对应语言的结构和句法，并且对文本进行分析来定位字。

字分离器可以一边接收一个字符流，一边发出另一个字符流。为了避免代码页(Code Pages)和其他双字节字符集(Character-set)所引起的问题，索引服务器使用单一代码(Unicode)来存储所有它的索引数据。当确定了一种语言后，系统将装载对应的字分离器。

(3) 规范化(Normalization)。索引的最后一步是文本规范化。从以上步骤中得到的单词对用户而言并不全部有用，有一些例外词或称干扰词不应包含在索引中，如中文里的“的”、“地”、“了”、“我”、“这个”和英文中的 I、you、and、of 等。规范化过程将“净化”由字分离器发来的文本，把数据以一致的表示方式放入索引中。

2. 查询过程

查询过程是索引服务真正处理用户请求的工作阶段。查询存在于浏览器和 Web 服务器之间，最基本的查询表查询方式的工作过程如图 10-2 所示。

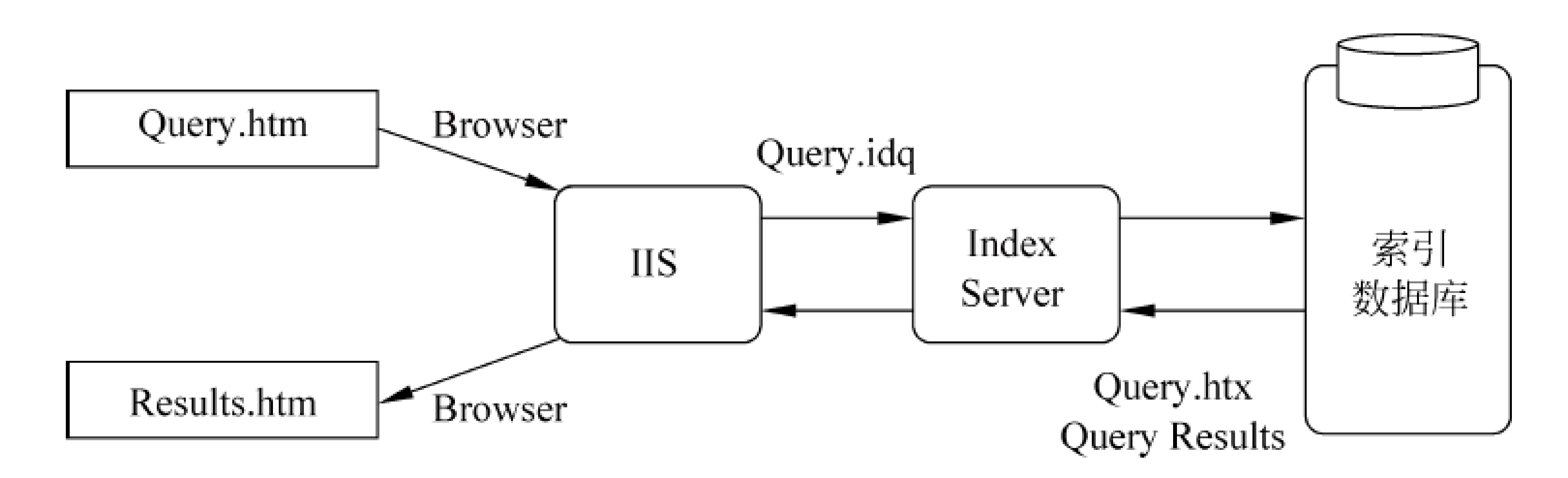


图 10-2　查询表查询方式的工作过程

查询基本流程如下：

(1) 浏览器连接到服务器，返回一个查找表格。用户填写这个查找表格，其中包括查询关键词或关键词的逻辑组合，然后单击【确定】按钮，把查询传送回服务器中。

(2) 查询表单以 Internet 数据查询文件(IDQ 文件)的形式发送到 Internet 信息服务器(IIS)，服务器检查到 IDQ 文件的引用，并把查询发给索引服务器。

(3) 索引服务器检查 IDQ 文件和查找表格中的内容，在其编录文件中查询相应关键词，找到含有这些关键词的文档。

(4) 索引服务器接受从索引返回的查询结果，IDQ 文件中的一行指定了一个 HTX 文件，用于对输出进行格式编排。

(5) 使用 HTX 文件中的查询结果和内容，索引服务器建立一个 HTML 结果页，该结果页传送回 Internet 信息服务器(IIS)，最后传回浏览器中。



10.2.3 微软索引服务的特点

微软索引服务具有如下特点。

（1）索引服务能够提供对多种格式文件的全文检索功能。默认情况下，下列类型的文档能够被索引：

- HTML 文档；
- 文本（txt）文档；
- Microsoft Office 95 和更高版本；
- Internet 邮件和新闻。

此外，安装相应文档过滤器的文档类型也能够进行索引。

（2）完全文本索引。可以根据一系列字或短语，甚至一个完整的句子进行搜索。

（3）根据性质查询。可以搜索存储于文件中的性质，如作者、专题、文件大小、日期等。

（4）模糊查询。可以使用通配符（Wildcards）和各种表达式来匹配所需要的查询。

（5）高级搜索功能。可以合并以上的所有特征来进行查询，包括字和字之间的接近位置，比较操作符（＜、＝、＞），和布尔逻辑（and、or、not）。

（6）可定制查询表格。可以预先定义常用的查询，并且创建定制的搜索和结果页。

（7）自动维护（Zero Maintenance）。当文档被改变、加入或删除时，索引服务器将自动更新。

（8）安全机制。用户仅能浏览被授予浏览权限的文档。

10.2.4 索引服务的系统需求

索引服务的最低硬件配置与 Microsoft Windows Server 2003 相同。索引服务的性能会受计算机系统资源的影响。同时，索引和搜索引擎的性能还取决于被索引文档的大小及数量多少，以及提交查询的速率和查询的复杂程度。如果同时进行的查询不是太多，满足 Windows Server 2003 最低硬件配置的计算机也能很好地处理查询。如果文档数目非常大，内存不足会影响索引性能。如果运行索引服务时系统性能很低，可以修改【索引服务用法】对话框中的选项调整性能。

表 10-1 显示了根据索引的文档数而推荐的内存配置。

表 10-1　索引服务内存配置

索引的文档数量	最小内存/MB	推荐内存/MB
少于 100 000	64	64
100 000～250 000	64	64～128
250 000～500 000	64	128～256
500 000 或更多	128	256 或更多



注意：编入索引的文档总体大小和正在使用的文件系统类型会影响存储索引服务的数据所需的磁盘空间大小。在 FAT 文件系统上，分类需要的空间加上临时工作空间大约是被索引文件总量的 30%。在 NTFS 文件系统上，需要的空间大约是索引的文件总量的 15%。

10.3　管理索引服务

10.3.1　索引服务的安装和启动

1. 安装

在默认情况下，索引服务在 Windows Server 2003 系统中已经安装但没有运行。如果本地计算机未安装索引服务，可用如下方法添加索引服务组件：

（1）依次选择【开始】→【设置】→【控制面板】命令，打开【控制面板】窗口。

（2）双击【添加/删除程序】快捷方式，打开【添加或删除程序】对话框。

（3）单击【添加/删除 Windows 组件】图标，打开图 10-3 所示的【Windows 组件向导】对话框。

（4）在【组件】列表框中，选中【索引服务】复选框，单击【下一步】按钮，出现安装信息。

（5）等待安装完成之后单击【完成】按钮，如图 10-4 所示。

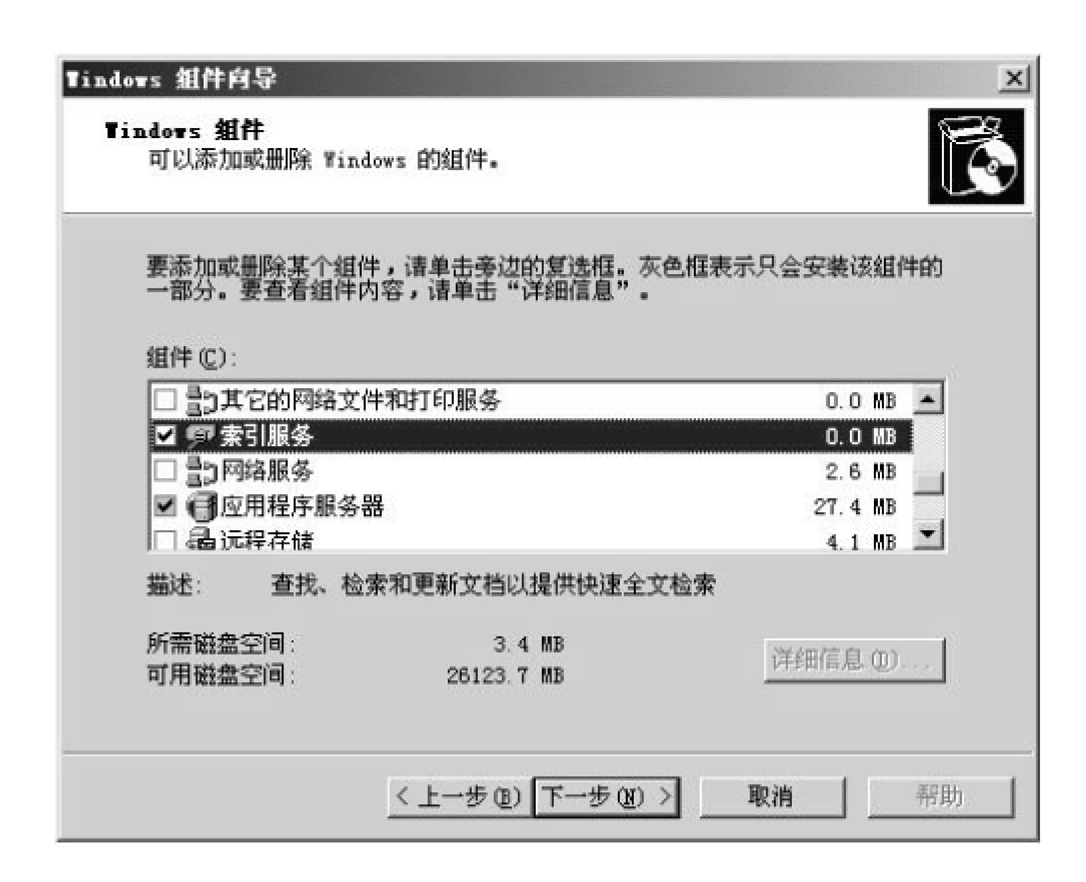


图 10-3　【Windows 组件向导】对话框



图 10-4　【完成"Windows 组件向导"】对话框

提示：上述步骤完成之后，在主机的【服务】窗口中便有了 Indexing Service（索引服务）服务项，在【计算机管理器】窗口中也多出一个【索引服务】节点。

2. 启动

默认情况下，索引服务在 Windows Server 2003 系统中并未启动。若此时使用索引服务查询，将收到索引服务未启动的错误提示对话框（错误 80041820-服务没有运行），如图 10-5 所示。



图 10-5　错误提示对话框





启动索引服务的具体步骤如下：

（1）依次选择【开始】→【程序】→【管理工具】→【服务】命令。

（2）在打开的【服务】窗口中选中 Indexing Service 服务项，如图 10-6 所示。

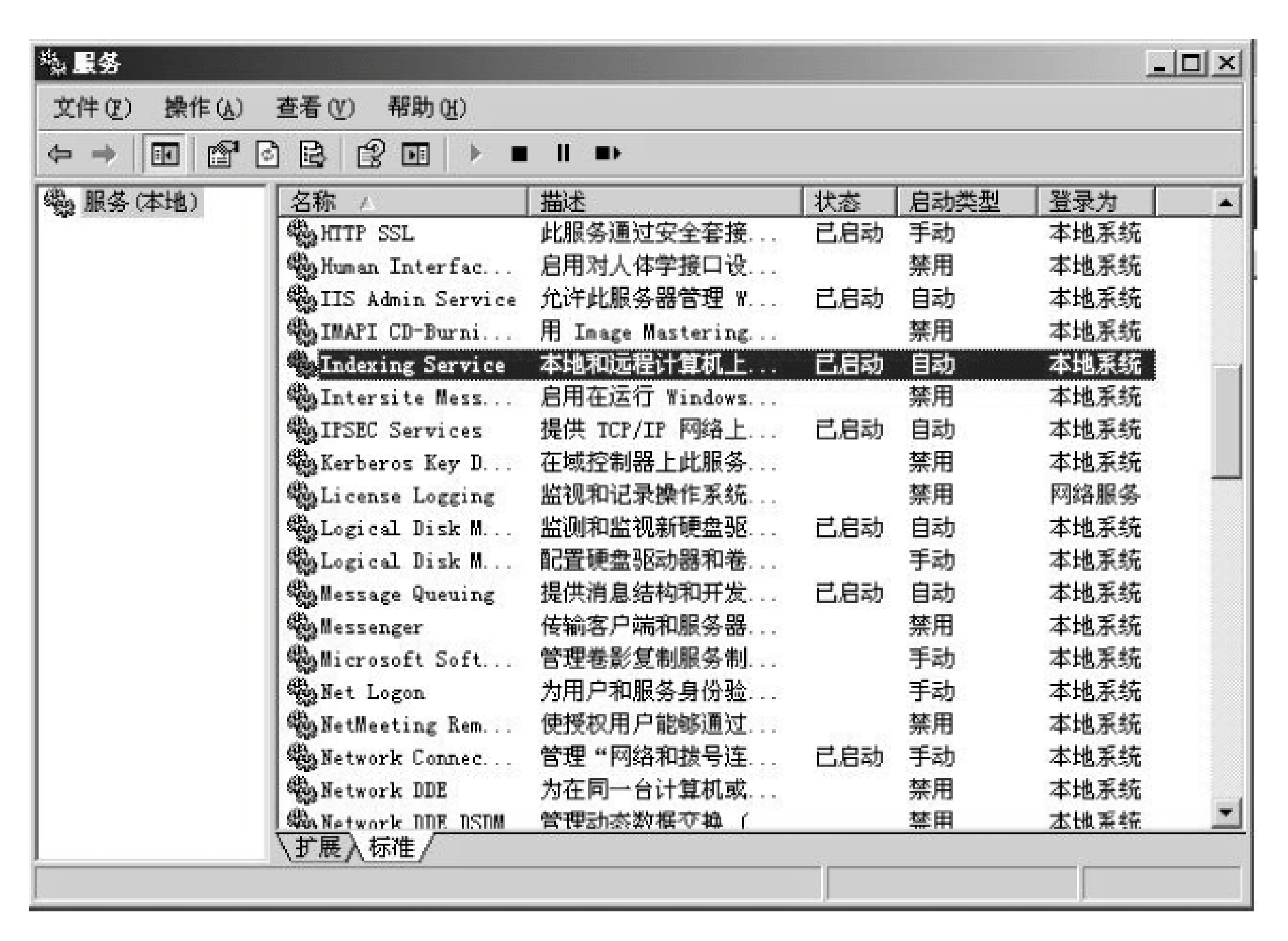


图 10-6 【服务】窗口

（3）在菜单栏中打开【操作】菜单，选择【启动】命令。此时，Indexing Service 服务项的状态变为“已启动”。

技巧：为使索引服务能跟随 Windows Server 2003 系统一同启动，可将其启动类型更改为“自动”。具体操作步骤如下：

① 在【服务】窗口中选择 Indexing Service 服务项。

② 在菜单栏中打开【操作】菜单，选择【属性】命令，出现如图 10-7 所示的【Indexing Service 的属性】对话框。在【常规】选项卡的【启动类型】下拉列表框中选择【自动】选项。



图 10-7 【Indexing Service 的属性】对话框

③ 单击【确定】按钮，设置完成。





10.3.2　配置索引服务

索引服务安装后，所有的操作都是自动完成，可以连续运行并且几乎不需要维护，一般不对其进行过多管理。需要更改的设置有如下几处。

1. 使索引服务能支持更多文件

在默认设置下，索引服务只支持具备相应筛选器的文档类型。为让其能够支持更多的文件，应进行如下设置：

(1) 打开【计算机管理】窗口，在控制台树中选择【索引服务】节点下相应编录节点。

(2) 选择【操作】→【属性】命令，在打开的【属性】对话框中，选择【生成】选项卡，如图 10-8 所示。

(3) 如果要索引未知文件扩展名的文档，选中【含有未知扩展名的索引文件】复选框，索引服务将提取文档中所有的内容和属性类型。

技巧： 若要使节点下的各编录使用与服务相同的设置，选择【继承服务的以上设置】复选框。

2. 生成摘要

要让索引服务在查询结果列表中产生文档的摘要，在【生成】选项卡中选中【生成摘要】复选框即可，如图 10-8 所示。在【最大尺寸(以字符为单位)】数值框中，可以设置摘要内容的大小限制。

3. 自动添加网络共享别名

具体操作步骤如下：

(1) 打开【计算机管理】窗口，在控制台树中选择相应的编录节点。

(2) 选择【操作】→【属性】命令，在打开的【属性】对话框中选择【跟踪】选项卡，如图 10-9 所示。



图 10-8　【生成】选项卡



图 10-9　【跟踪】选项卡

(3) 要使索引服务将共享目录的共享名当作该目录的别名，选中【自动添加网络共享别名】复选框。要使节点下的各编录使用与服务相同的设置，选中【继承服务的以上设置】复选框。



4. 索引 Web 服务器

在【属性】对话框中选择【跟踪】选项卡，在【WWW 服务器】列表中选择要索引的 Web 服务器，如图 10-9 所示。如果计算机上没有安装 Internet 信息服务器(IIS)，则 WWW 服务器控件显示为“不可用”。

注意：为使以上更改生效，更改之后必须重新启动相应编录和索引服务。

10.3.3 索引和编录状态

1. 索引服务状态

Microsoft 管理控制台(MMC)的详细信息窗格中列出了索引服务不同元素的状态，如图 10-10 所示。对于每个编录节点，显示如下信息。

- 编录。编录名。
- 位置。编录的路径和文件夹名。
- 大小(Mb)。以兆位表示的编录大小。
- 文档总数。已编入索引的文档总数。
- 待索引的文档。待编入索引的文档数。
- 延迟建立索引。需要编入索引但因为正在使用而暂时无法进行的文档数。
- 词列表。内存中的字数。
- 保存的索引。编录中已保存的索引数。
- 状态。编录的状态。

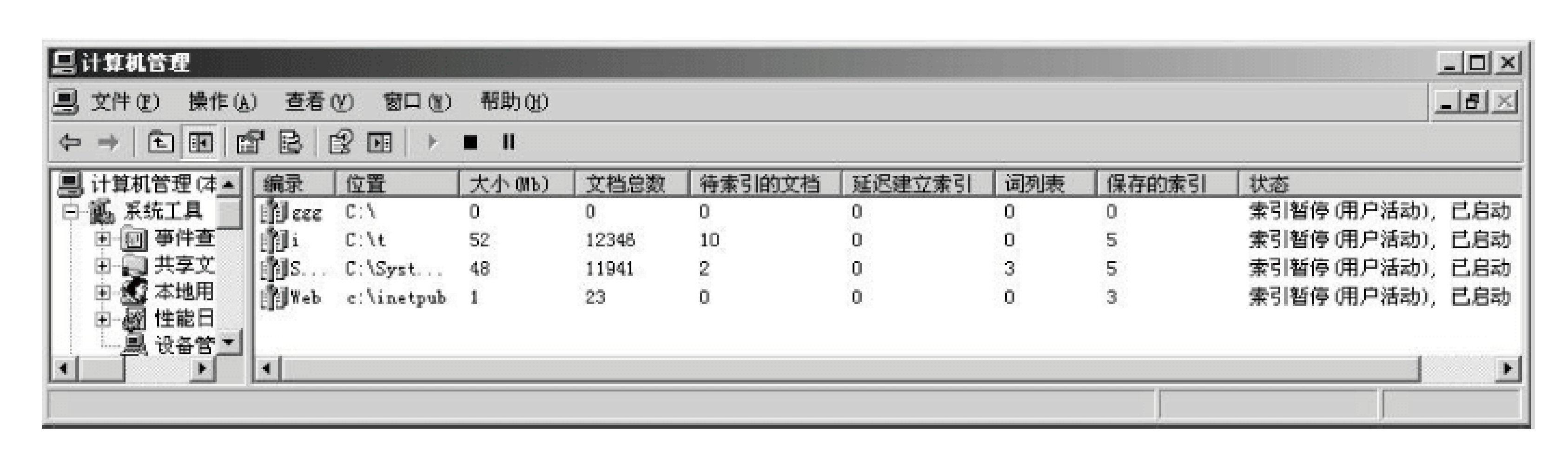


图 10-10 【Microsoft 管理控制台】窗口

2. 编录状态

在展开编录节点时，将出现【目录】节点、【属性】节点和【查询编录】查询表。当展开【目录】节点时，详细信息窗格会显示一个列表，列出编录作用域中所有目录、每个目录的别名，并指出目录是否将被索引。

对于在信息窗中的每个选项，其意义如下。

(1) 目录。物理目录列表。这些目录下的所有文档均编入索引。与虚拟目录对应的项目用特殊的文件夹图标标记。有三种目录显示在详细信息窗格中，如图 10-11 所示。

- 物理目录，用黄色的文件夹图标表示。
- 影子目录，用深黄色文件夹图标表示。影子目录是被列出别名的共享目录。
- 虚拟目录，用文件夹和地球图标表示。虚拟目录指代一个虚拟根。





图 10-11　目录状态

（2）别名。目录的服务器名和路径。别名在查询结果列表中被返回给从远程计算机上提交查询的用户。该栏可能为空。

（3）包括到编录中。“是”表示该目录及其所有子目录将包括到编录作用域中并将建立索引。“否”意味着目录及其所有的子目录不包括在编录作用域内并且不被索引。

3. 属性状态

当单击相应编目下【属性】节点时，详细信息窗格显示在已安装的筛选器中标识的所有属性的列表。详细信息窗格包括以下内容，如图 10-12 所示。



图 10-12　属性状态

- 属性集。一组属性的属性数。
- 属性。属性的十六进制或字符串 ID。
- 好记的名称。容易理解的属性名。
- 数据类型。属性的数据类型。
- 高速缓存大小。缓存中分配给属性值的空间大小。
- 存储级别。属性值保存处的缓存级别。

10.3.4　调整索引服务性能

索引服务效率的高低取决于使用索引服务的频繁程度，所以应根据服务器不同的使用方式来调整索引服务的性能。



具体操作步骤如下：

（1）单击【索引服务】节点，选择【操作】→【所有任务】→【调整性能】命令，如图 10-13 所示。

（2）在弹出的【索引服务用法】对话框中，根据服务器当前承担的索引工作量和服务性质选择最适合的索引服务用法，如图 10-14 所示。可选用法有专用服务器、经常使用，但没有专门用于这个服务、偶尔使用、从不使用和自定义。它们所对应的规划索引工作量依次递减，对于一般的包含索引功能的 Web 服务器，指定“偶尔使用”用法即可满足需求。



图 10-13 【调整性能】命令



图 10-14 【索引服务用法】对话框

（3）选择【自定义】单选按钮后，可单击【自定义】按钮，在弹出的【所需性能】对话框中进行自定义配置，如图 10-15 所示。

（4）在【所需性能】对话框中，可以自定义为索引和查询服务预留的资源。将【索引】滑块移到“迟缓”以延缓索引或移到“立即”以立即索引新文档和更改过的文档。迟缓索引使用较少的资源，立即索引将使用尽可能多的计算机资源。若想一次处理少量查询，可将【查询】滑块移到“低负载”；若需要同时处理大量的查询，可将滑块移到“高负载”。低负载使用较少资源，而高负载使用较多的系统资源。该对话框中的两个滑块为灵活配置索引服务器提供了选择，应该据服务器的硬件水平和系统的实际需要配置这些选项。

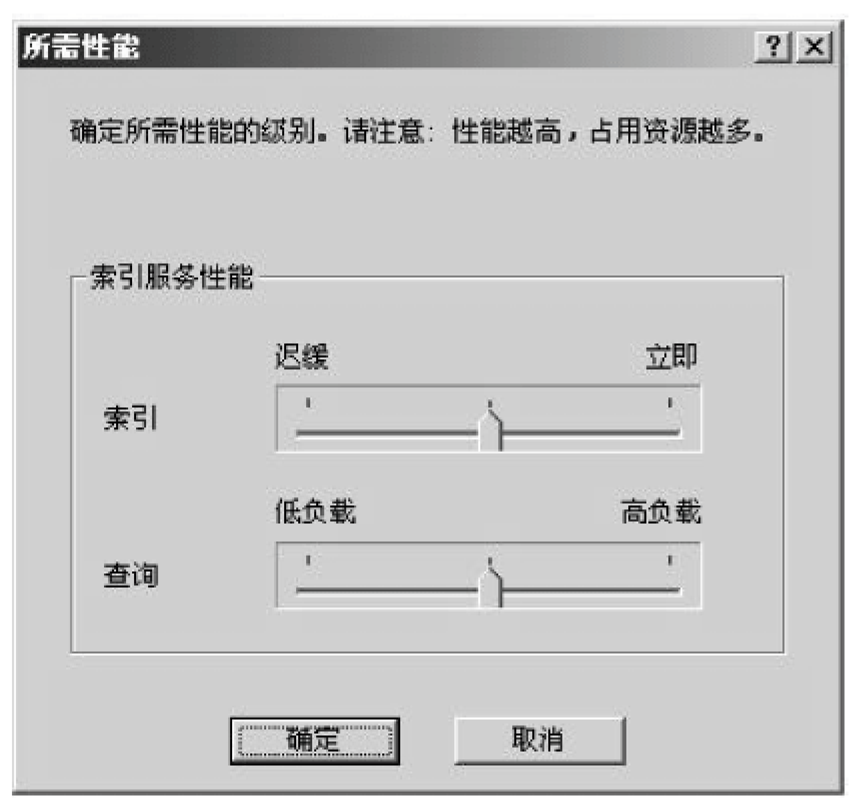


图 10-15 【所需性能】对话框

（5）单击【确定】按钮返回，并重新启动索引服务。

注意：调整索引服务性能之前，应先停止索引服务。

10.3.5 设置文档属性

文档属性代表了文档的特征，例如创建日期、作者姓名和文档大小。属性值是特定



档案的特定信息。有些属性值由创建文档的程序自动设置，而有些属性值则由用户输入。有些文档，例如用 Microsoft Office 创建的文档或 HTML 文档，用户可以创建其自定义属性。

所有文档的属性和属性值都同文档内容一道被编入索引并且可以被搜索。多数属性还可以显示在搜索结果的列表中。但是，某些属性在文档被索引时必须被存储在属性缓存中，否则索引服务将无法找到它们，也就无法在搜索结果中显示。如果默认的选择不符合要求，那么可以自定义指定那些特定的要保存到属性缓存中的属性。

设置文档属性的步骤如下：

（1）打开【计算机管理】窗口，在控制台树中的相应编录下单击【属性】节点。

（2）在信息窗的【属性集】属性列中，单击想要添加到缓存中的属性的 ID。

（3）打开【操作】菜单，选择【属性】命令，弹出图 10-16 所示的【属性】对话框。

（4）选中【高速缓存】复选框。

（5）在【数据类型】下拉列表框中选择要添加的数据类型。

（6）对于可变大小的属性，在【大小】数值框中，设置属性的大小（以字节为单位）。

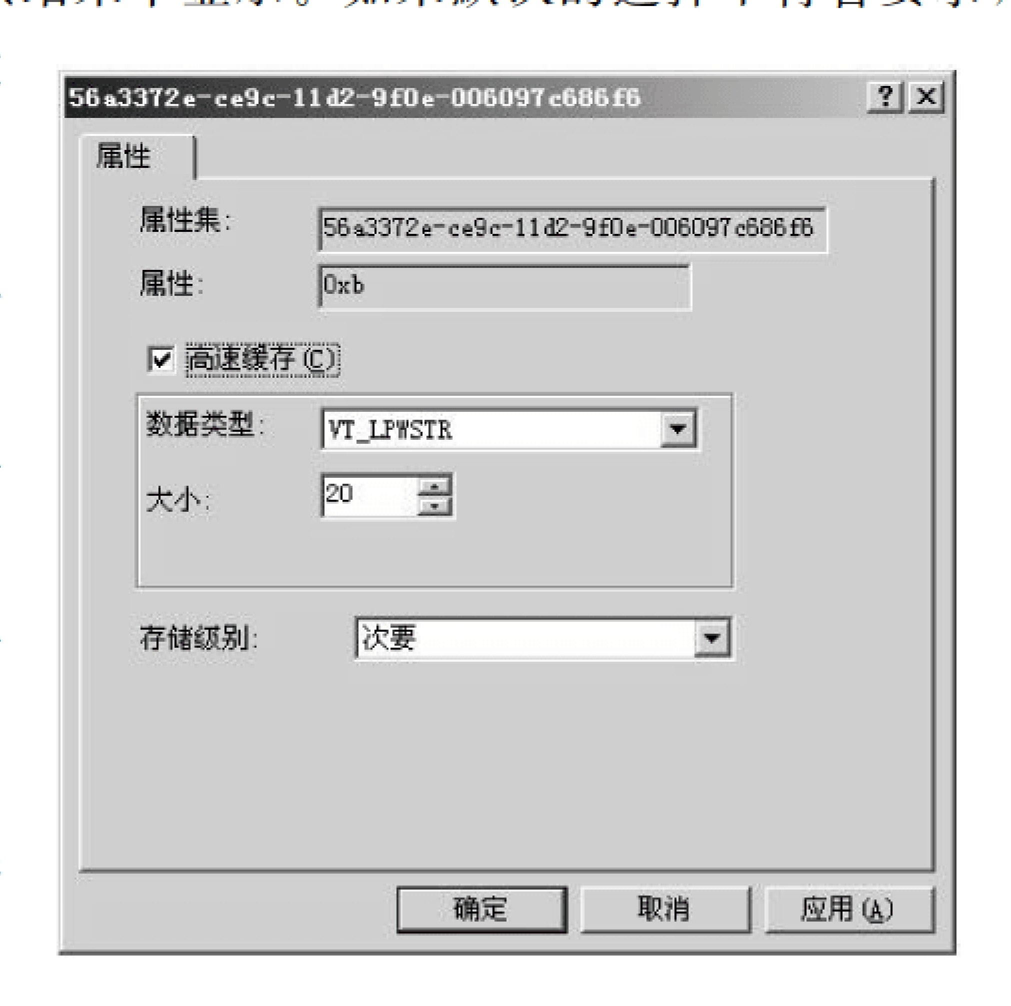


图 10-16　【属性】对话框

注意：属性大小是需要用来存储属性值的字节数。属性的大小可以是固定的，也可以是可变的。如果给编录添加了固定大小的属性，索引服务将为属性设置适当的大小。对于可变大小的属性，用户可选择其大小。每一文档的每个选定属性的全部值都将存储。设置的大小会影响到目录所需磁盘空间的大小和处理查询所花费的时间。如果设置得较大，目录将需要更多的磁盘空间，但可提高查询性能；如果设置得较小，将节省磁盘空间，但可能会以降低性能为代价。

每次做出更改时，必须对更改进行一次完全扫描以使其对所有文档均生效。

10.3.6　禁止索引指定的目录和文档

1. 禁止索引 FAT 格式存储的目录和文档

对于采用 FAT 格式存储的目录和文档，可将这些目录和文档所在的目录添加到编录中并将【包括在索引中吗?】选项设置为“否”。具体操作步骤如下：

（1）打开【计算机管理】窗口，在控制台树中的相应编录下单击【目录】节点。

（2）选择【操作】→【新建】→【目录】命令，弹出图 10-17 所示的【添加目录】对话框。

（3）在【路径】文本框中输入要禁止索引的目录路径，或者单击【浏览】按钮查找目录。

（4）在【包括在索引中吗?】选项区域中选中【是】单选按钮将目录包含到编录中，或者选





图 10-17 【添加目录】对话框

中【否】单选按钮将目录排除在编录之外。

(5) 单击【确定】按钮完成设置。

技巧:也可修改已添加的目录,设置其是否可被索引。这可在编录节点的目录列表中双击需要暂停索引的目录,打开【添加目录】对话框进行设置。

2. 禁止索引使用 NTFS 文件系统的目录和文档

在使用 NTFS 文件系统的分区中,可以应用上述同 FAT 文件格式的设置,也可以在文件夹的属性管理中设置相应的文件夹和文档是否能被索引。操作步骤如下:

(1) 在【Windows 资源管理器】窗口中,选择文档或文件夹。

(2) 打开【文件】菜单,选择【属性】命令,弹出图 10-18 所示的【文件夹属性】对话框。

(3) 选择【常规】选项卡,单击【高级】按钮,弹出图 10-19 所示的【高级属性】对话框。



图 10-18 【文件夹属性】对话框

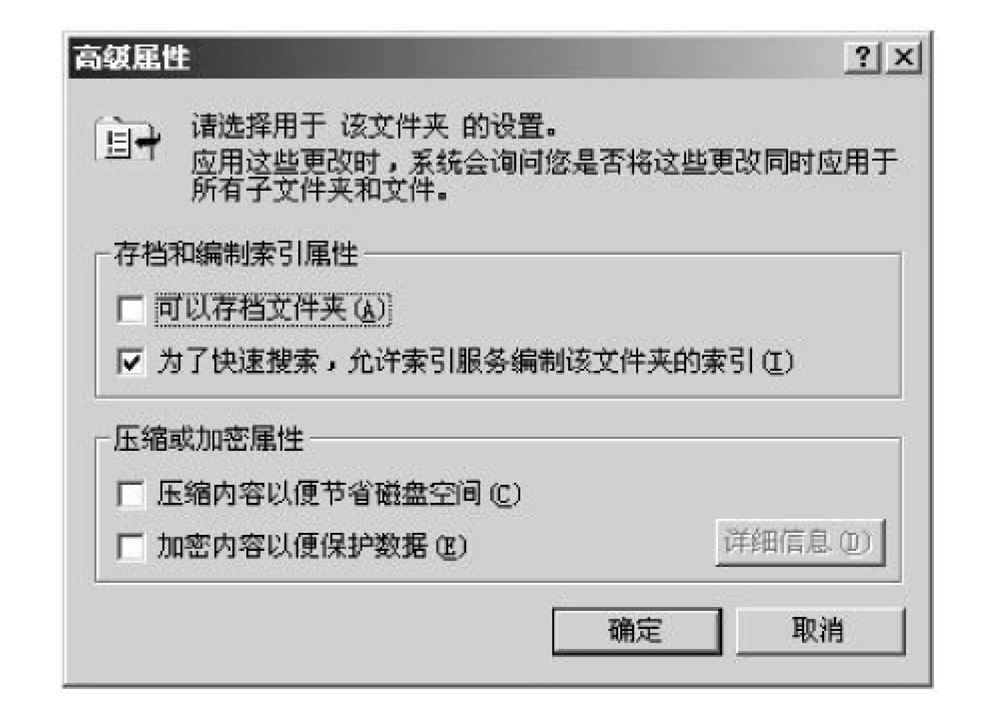


图 10-19 【高级属性】对话框

(4) 要禁止该文件夹或文档被索引,则取消选中【为了快速搜索,允许索引服务编制该文件夹的索引】复选框,单击【确定】按钮。



(5) 单击【应用】按钮，弹出图 10-20 所示的【确认属性更改】对话框，显示“只将该更改应用于该文件夹，还是同时应用于所有子文件夹和文件?”询问，选中下方相应的单选按钮，单击【确定】按钮返回。

注意：若要禁止索引某个指定的磁盘分区，其操作与上述文件夹操作类似，打开【本地磁盘属性】对话框，取消选中【允许索引服务编制该磁盘的索引以便快速搜索文件】复选框即可，如图 10-21 所示。

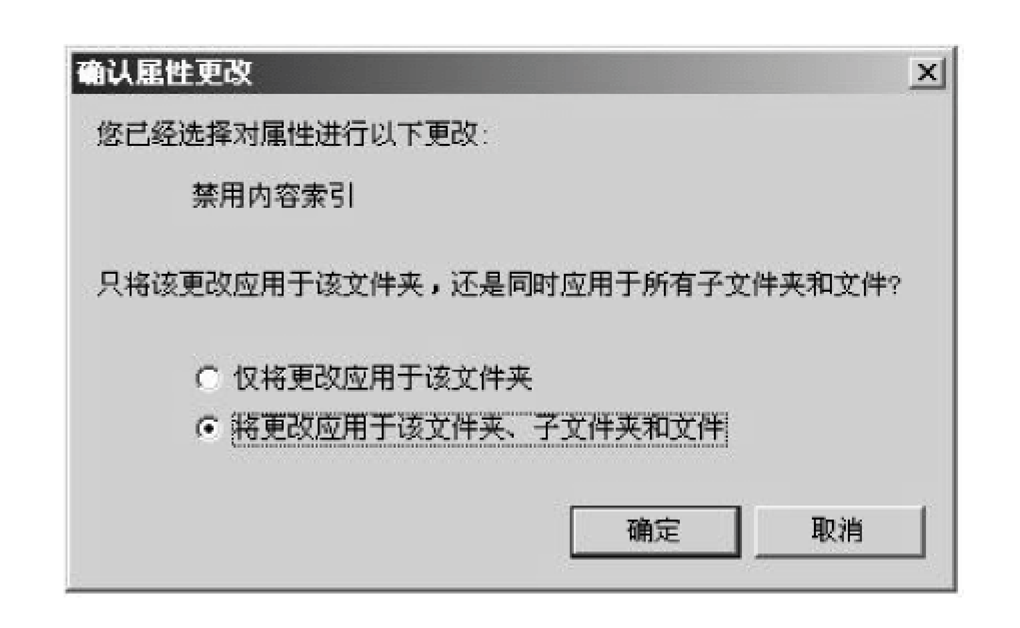


图 10-20 【确认属性更改】对话框

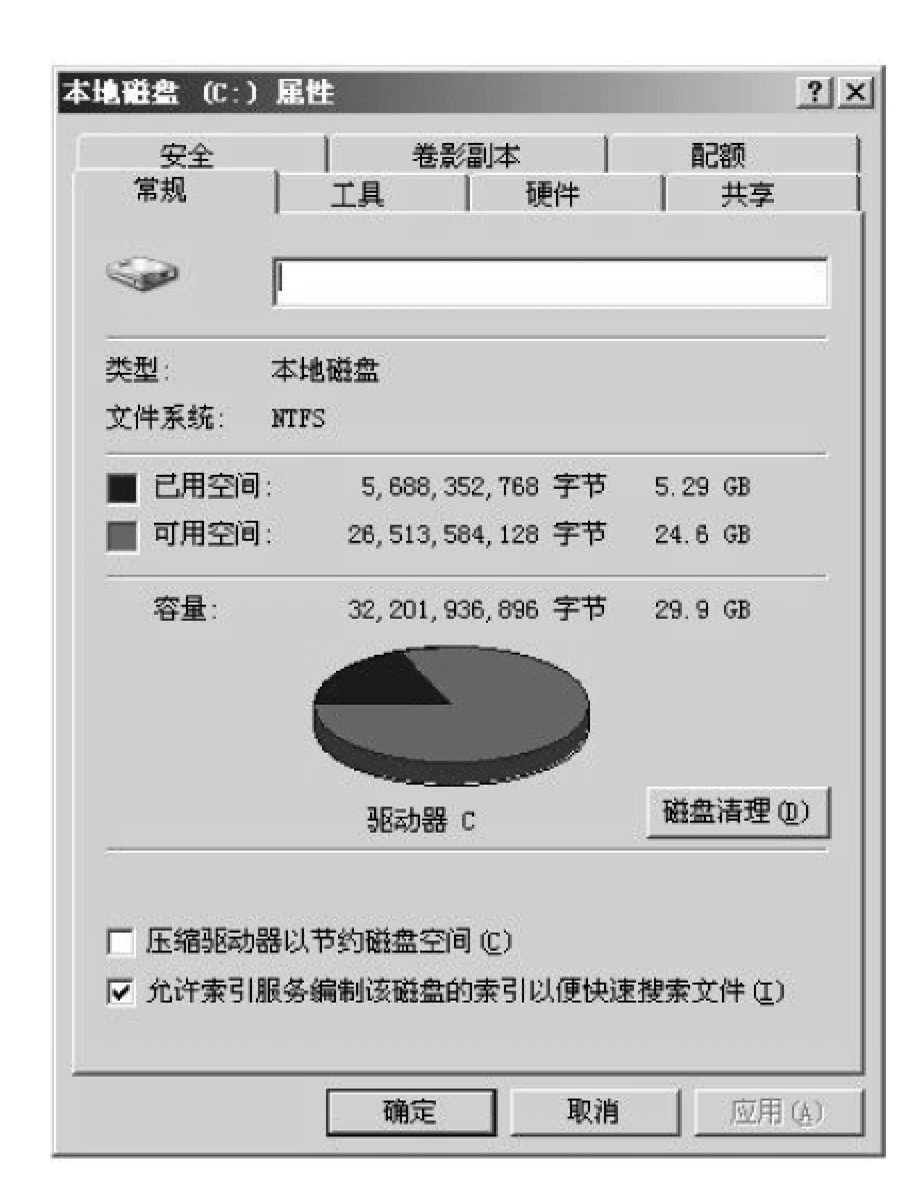


图 10-21 【本地磁盘属性】对话框

10.3.7 监视性能

使用 Windows Server 2003 中内置的性能监视功能可以监视索引服务的使用情况。具体操作步骤如下：

(1) 依次选择【开始】→【程序】→【管理工具】→【性能】命令，打开对应的【性能】窗口。

(2) 再创建新计数器集，并在打开的【添加计数器】对话框中添加与索引服务有关的计数器，如图 10-22 所示。

(3) 选择完毕后，单击【添加】按钮，然后单击【关闭】按钮，退回【性能】窗口，如图 10-23 所示。

表 10-2 和表 10-3 分别对相关计数器进行了说明。

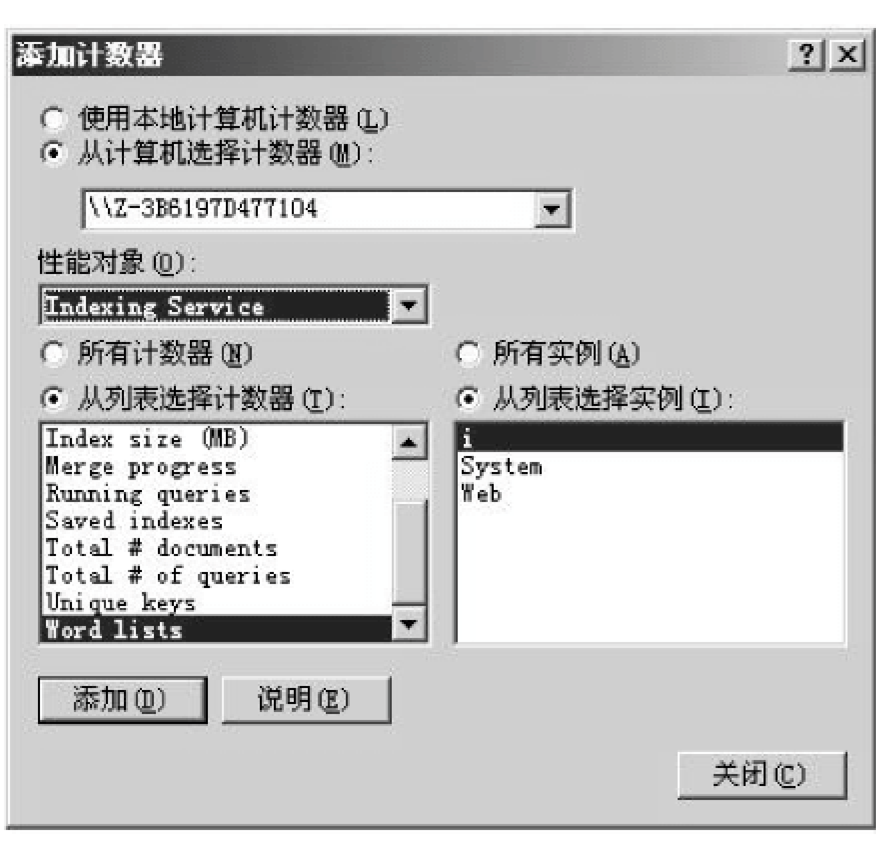


图 10-22 【添加计数器】对话框





图 10-23 【性能】窗口

表 10-2 和索引服务相关的性能计数器

计 数 器		说 明
# documents indexed	索引过的文档数	自从当前索引会话启动以来索引过的文档数。注意：这不包括在“索引服务”会话之前索引过的文档
Deferred for indexing	延迟建立索引	需要编入索引但因为文档正在使用而暂时无法完成的文档数
Files to be indexed	待索引的文档数	已知需要索引的最小文档数
Index size (MB)	索引大小(MB)	所有已保存索引的总大小(以兆字节为单位)
Merge progress	合并进度	完成合并的百分比
Running queries	运行中的查询	正在处理的查询数
Saved indexes	保存的索引	已保存索引的总数
Total # documents	文档总数	索引中已知的文档总数
Total # of queries	查询总数	在该索引会话中处理的查询总数
Unique keys	唯一关键字	索引中的唯一字的数量
Word lists	词列表	词列表总数

表 10-3 和索引服务筛选器相关的性能计数器

计 数 器		说 明
Binding time/(ms)	绑定时间(ms)	绑定到筛选器文件的平均时间(ms)
Indexing speed (MB/h)	索引速度(MB/h)	文档索引速度/(MB/h),不包括生成的摘要
Total indexing speed(MB/h)	总索引速度/(MB/h)	文档索引速度(MB/h),包括生成的摘要



10.4　建立和维护索引

10.4.1　添加和删除索引

1. 创建编录

默认情况下，Windows Server 2003 有 Web 编录和 System 编录。如果要对索引信息进行详细划分，可以规划多个不同编目。创建编录的方法如下：

(1) 打开【计算机管理】窗口。

(2) 在控制台树中单击【索引服务】节点。

(3) 选择【操作】→【新建】→【编录】命令。

(4) 在弹出的【添加编录】对话框中输入编录名称，如图 10-24 所示。单击【浏览】按钮，选择要放置该新类别的文件夹，即编录文件的储存路径。

(5) 单击【确定】按钮完成。

在添加编录后，必须将该编录的作用域所包括的目录添加进去才能进行索引服务。默认情况下，系统编录包含了所有本地存储器的全部目录，但不包括 Internet 临时文件和历史记录文件。可将目录添加到编录作用域，也可以将目录排除在索引之外。用户可根据自己的实际情况适当增减被索引的目录范围。

2. 添加目录

在编录中添加目录的方法如下：

(1) 打开【计算机管理】窗口。

(2) 单击相应编录节点。

(3) 选择【操作】→【新建】→【目录】命令。

(4) 在弹出的【添加目录】对话框中指定目录的路径和别名，如图 10-25 所示。

(5) 单击【确定】按钮完成。



图 10-24　【添加编录】对话框



图 10-25　【添加目录】对话框

当目录添加到编目中之后，索引服务自动进行扫描和索引过程，无须人工参与。如果不想索引某些特定的文档，把该目录添加到【目录】列表中，并在【包括在索引中吗?】选项区域



中选中【否】单选按钮。这样，该目录就从编录中排除，不再对其进行索引。也可以使用通配符限制编录的作用域。

3. 删除编录和目录

要删除编录需先停止索引服务。操作步骤如下：

(1) 打开【计算机管理】窗口，在控制台树中单击【索引服务】节点。

(2) 选择【操作】→【所用任务】→【停止】命令。

(3) 单击要删除的编录，选择【操作】→【删除】命令。

(4) 在弹出的确认对话框中单击【是】按钮，如图10-26所示。

(5) 重启动索引服务。

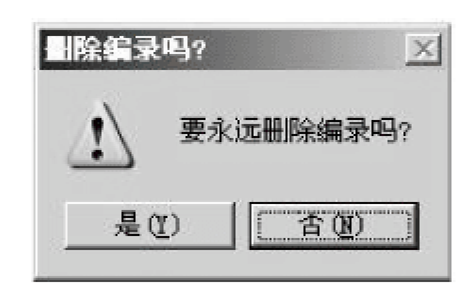


图10-26 确认对话框

从编录中删除目录同删除编录类似。在控制台树中的相应编录下单击【目录】节点，选择要删除的目录，再打开【操作】菜单，选择【删除】命令。

注意：在做删除操作前应先停止索引服务，操作完成后应重新启动索引服务。

10.4.2 暂停、停止、启动索引服务和编录

打开【计算机管理】窗口，在控制台树中选中【索引服务】节点，打开【操作】菜单中的【所有任务】子菜单，可以分别使用其中的【启动】、【停止】、【暂停】命令进行必要的操作。也可使用工具栏中的按钮来操作，如图10-27所示。

图10-27 【启动】、【停止】、【暂停】按钮

暂停、停止或启动特定的编录，单击此编录，其后操作同上所述。

注意：当索引服务暂停时，详细信息窗格中的状态栏显示"只查询"。索引服务暂停时，不进行文档索引，但仍然处理查询。

10.4.3 索引扫描

扫描是清点目录以便确定应该为哪些文档建立索引的过程。根据需要，索引服务会自动执行扫描。

1. 完全扫描和增量扫描

扫描分为完全扫描和增量扫描两种，完全扫描列出编录中全部目录所包含文档的清单，并将其添加到索引文档列表中。

在下列情况中，索引服务对计算机上的磁盘驱动器进行完全扫描：

- 索引服务在安装后第一次运行时。
- 将文件夹添加到编录中时。
- 发生严重错误时，作为故障恢复的一部分。

而当索引服务重新启动时，将通过增量扫描检测所有文档发生的变化，从而可以更新索





引。如果索引服务丢失相应数据，也会执行增量扫描。

2. 手动扫描

一般情况下，索引服务自动进行扫描工作。但是在某些情况下，有必要手动启动对索引目录的完全扫描或增量扫描。在下列情况下应该手动启动扫描：

- 安装了新的筛选器、删除了筛选器或修复了筛选器的注册信息。
- 更改了摘要的大小。
- 更改了未知文档扩展名的索引。
- 添加了新的断词软件。
- 将属性添加到属性缓存。
- 更改了属性缓存中属性的类型或大小。
- 添加了新的语言。
- 编辑了例外词表。

手动扫描的方法如下：

(1) 打开【计算机管理】窗口，在控制台树中的相应编录下单击【目录】节点。

(2) 在信息窗中单击要扫描的目录。

(3) 打开【操作】菜单，选择【所有任务】→【重新扫描(完全)】命令进行完全扫描，或者选择【重新扫描(增量)】命令进行增量扫描，如图10-28所示。

(4) 在确认对话框中单击【是】按钮开始扫描。



图 10-28 【操作】菜单

10.4.4 合并索引

当索引被保存到磁盘后，就是已保存的索引。已保存的索引信息按高度优化的压缩格式存储，该格式可实现对搜索的快速响应，并且能充分地节约系统资源。合并索引就是将已保存各处的索引中的数据合并到永久的主索引中，以便对查询进行高效率的解析。

索引服务会自动将临时索引合并为一个主索引，并删除多余的数据，释放系统资源，这样查询文档会执行得更快。在合并过程中，并不会影响到对已建立索引的文档进行查询。

合并索引需要处理器长时间高负荷工作。在合并时，查询的速度可能会明显减慢，但在合并后查询将变得更快。如果对编录中包含的文档进行了大的改动，可以手工启动合并。

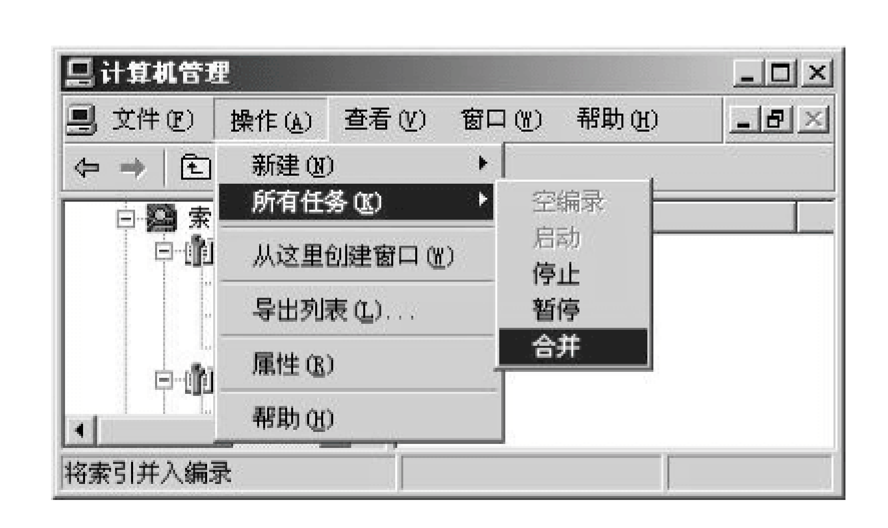


图 10-29 【合并】命令

手动合并编录中的临时索引，方法如下：

(1) 打开【计算机管理】窗口，在控制台树中单击相应的编录节点。

(2) 选择【操作】→【所有任务】→【合并】命令，如图10-29所示。

(3) 在【合并目录】确认对话框中单击【是】按钮，开始合并。



10.5 索 引 查 询

使用索引查询，可以通过输入文档内容或其属性（例如文档名或作者）来搜索文档，也可以查找属性值与给定条件相匹配的文档。微软索引服务器还提供了查询语言来检索特定文档，查询结束后，索引服务将返回符合查询条件的文档列表。

10.5.1 查询方式

1. 使用“搜索”功能搜索

使用【开始】菜单上或文件夹中的“搜索”功能搜索，其步骤如下：

（1）选择【开始】→【搜索】→【文件或文件夹】→【其他搜索选项】→【所有文件和文件夹】命令。

（2）在弹出的窗口的文本框中输入该文件或文件夹的全名或部分名称，或者输入文件中包含的字或词组，如图 10-30 所示。



图 10-30 【搜索结果】窗口

（3）单击【搜索】按钮开始搜索。

技巧： 文本框下面其余的选项可以帮助进一步缩小搜索范围提高搜索速度，或者用其他的相关信息来搜索。

- 在【查找范围】列表框中选择想要查找的驱动器、文件夹或网络。



- 单击【什么时候修改的?】按钮,可查找在某个特定日期或两个特定日期之间创建或修改的文件。
- 单击【大小是?】按钮,可查找具有指定大小的文件。
- 单击【其他高级选项】按钮,可指定附加的搜索条件。

2. 使用索引服务查询表格搜索

查询表包含在索引服务的每个相应的编录中,如图 10-31 所示。通过查询表可以使用查询语言的所有功能运行任何类型的查询。操作步骤如下:

(1) 打开【计算机管理】窗口,在左侧控制台树中选择相应的编录节点。

(2) 单击该编录下【查询编录】节点,打开如图 10-31 所示的【索引服务查询表格】窗口。



图 10-31　【索引服务查询表格】窗口

(3) 在【请在下面输入自由文本查询】文本框中输入关键词或查询语句,单击【搜索】按钮。

提示: 一般情况下,搜索文本文档使用标准查询即可。若要使用"索引服务查询语言"功能,则需选中【高级查询】单选按钮。

3. 使用 Web 浏览器提交查询

微软索引服务器可以索引存储在 Internet 信息服务器(IIS)中所有文档的内容和属性,能够通过 Internet 信息服务器(IIS)与索引服务器的交互,为本地的网络服务器建立一套独立的站内搜索系统。

当配置好相关服务以后,通过填写一个查询表格来输入查询条件,使用 Web 浏览器来



搜索服务器，Web 服务器把查询表格传递给索引服务器，并由索引服务器的查询机制找到相关的文档，然后把结果以 Web 页的格式返回给客户端。除了 HTML 和文本文件外，索引服务器还可以索引特定格式文档的所有文本内容和属性值，例如由 Word 或 Excel 创建的文档。

索引服务器允许用户制定查询表格来建立本地搜索。这种查询表格由标准 HTML 语言创建，如果自己会创建 Web 页，就可以修改制作简单的查询表格，如图 10-32 所示。



图 10-32　一个简单的 Web 查询页

索引服务返回符合查询条件的文档列表，也就是结果集。结果集中的每一项均是查询的一次命中。索引服务可以根据符合查询的程度，对命中项进行排序，还可以根据文档属性值对结果进行多级排序。在 Web 页上，可以限制返回结果的最大命中数。例如，一组 200 个命中结果的结果集可分 10 页显示，每页 20 个命中结果。

要使网站内容能被有效索引到，需要把存储网页信息的虚拟文件夹加入到编录中。具体方法如下：

(1) 依次选择【开始】→【程序】→【管理工具】→【Internet 服务管理器】。

(2) 在弹出的窗口左侧控制台树中选中相应的网站节点。

(3) 选择【操作】→【属性】命令。

(4) 在弹出的【属性】对话框的【主目录】选项卡中，选中【索引资源】复选框，如图 10-33 所示。

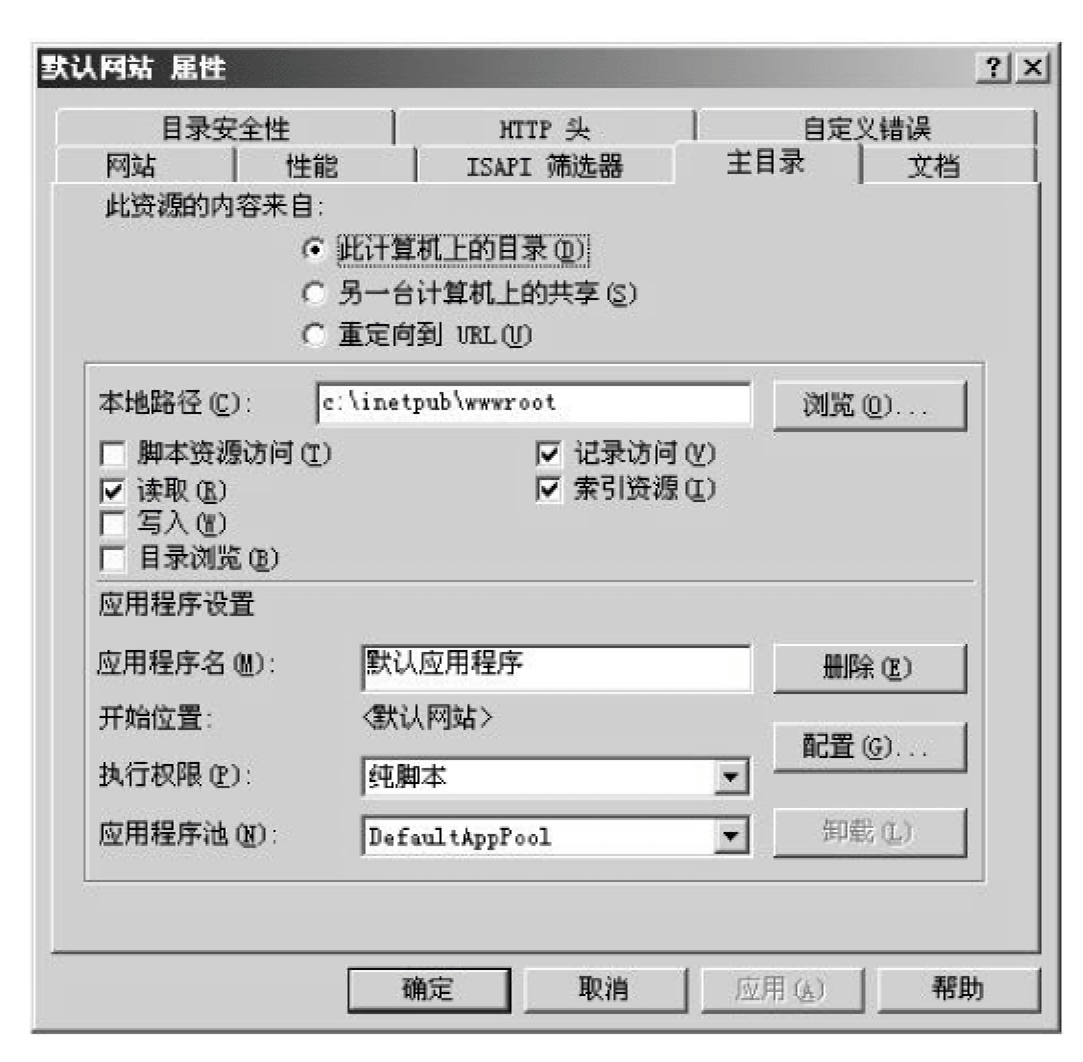


图 10-33　【主目录】选项卡



（5）单击【确定】按钮。

对于站点属性以下的目录、虚拟目录，均可用此方法进行索引或解除索引。同时应保持【Web 服务扩展】窗口中 Indexing Service 服务被允许，如图 10-34 所示。



图 10-34 【Web 服务扩展】窗口

10.5.2 查询语言查询

在索引服务的查询表格和 Web 查询页面中，可以使用微软索引服务器提供的查询语言来进行高级查询。也可通过在查询表格中输入单词或短语，然后单击按钮来执行查询。下面给出查询语言的通用规则：

- 连续的单词作为短语对待，它们在匹配文档中必须以相同的顺序出现。
- 查询不区分大小写。
- 可以搜索任何单词，但不包括在例外列表中列出的单词（对于英语，包括 a、an、and、as 和其他一些单词），它们在查询中将被忽略。
- 在例外列表中的单词在短语中将作为占位符对待，用来进行相似查询。例如，如果查询 Word for Windows，结果将给出 Word for Windows 和 Word and Windows，因为 for 是一个在例外列表中出现的虚词。
- 标点符号在搜索时将被忽略，如句号“.”、冒号“:”、分号“;”和逗号“,”。
- 要搜索包含引号的单词或短语，应先用引号把整个短语括起来，并用两遍引号括住该单词。例如，World-Wide Web or “Web”将搜索 World-Wide Web or “Web”。
- 时间和日期的格式是 yyyy/mm/dd hh:mm:ss 或 yyyy-mm-dd hh:mm:ss。在秒数值之后，可指定三位数的毫秒值。例如，1997/12/8 13:10:03:452。
- 数字值可以是十进制或十六进制。十六进制值之前均有 0x。

查询语言的一般形式由几部分构成，分别是模式符号（如“@”、“#”、“$”）、属性名＋运算符＋属性值。

1. 模式符号

其中“@”符号用于词组查询，“#”符号用于常规表达式查询，“$”符号用于自由文本查询。“@”和“#”符号多用于文档属性的匹配查询。



2．属性名

系统中的所用文档都有其自身各类属性，来对应其所含的各项信息。用属性值查询，可以查找含有与所给标准相匹配的属性值的文件。可以用来查询的属性包括文件的基本信息（如文件名、文件大小）和 ActiveX 属性（包含在文档摘要中），ActiveX 属性由 ActiveX 应用程序创建并存储在文件中，如表 10-4 和表 10-5 所示。

表 10-4　所有文档可用的属性

属　性　名	说　　明
All	所有属性，包括 Contents。只用于文本查询，而不是数值查询
Contents	文档中的词和词组
Filename	文档名
Size	用字节表示的文档大小
Write	文档的最近一次修改的日期和时间

表 10-5　部分 ActiveX 属性

ActiveX 属性名	说　　明	ActiveX 属性名	说　　明
DocTitle	文档标题	DocKeywords	文档的关键字
DocSubject	文档主题	DocComments	文档的注释
DocAuthor	文档作者		

提示： ActiveX 属性值也可用于查询中。在 Web 站点中大多数 ActiveX-aware 应用程序创建的文档可以用表 10-5 中列出的属性查询。

注意： 属性名不区分大小写。在可查询的属性中有两个特殊的属性：Contents 和 All。Contents 属性指文档的内容。当在查询中指定 Contents 时，索引服务只搜索文档的内容。当在查询中指定 All 时，索引服务搜索文档的内容和属性值。如果在查询中不指定任何属性，索引服务将选择默认的 Contents 属性。

3．布尔和相近运算符

在内容和属性查询中都可以使用布尔运算符 and、or 和 not。使用 not 运算符只排除与前面内容限制匹配的文档。相近运算符 near 仅用于内容查询，如表 10-6 所示。

提示： 当在查询中使用 near 运算符时，如果词分别在文档中的 50 个单词以内，则文档匹配查询。词靠得越紧，在结果集中分配给文档的等级就越高。包含搜索单词较近的页的等级将大于或等于单词相隔较远的页的等级。如果是 50 个以上的分离词，则认为这些词的距离不够近，该文档将被指派为零级。near 运算符仅应用于词或词组的查询。

表 10-6　布尔和相近运算符范例

搜索内容	格　式	结　果
同一文档中有两个词条	red and dog 或 red & dog	既包含 red 又包含 dog 的文档
文档中有两个词条中的任何一个	red or dog 或 red | dog	包含单词 red 或 dog 的文档
包含前一个但不包含后一个词条	red and not dog 或 red &！dog	包含 red 但不包含 dog 的文档
与属性值不匹配的文档	not@size=100 或！@size=100	大小不等于 100 字节的文档
两个词条在同一文档中相距不远	red near dog 或 red ～ dog	在词 dog 附近有 red 的文档

布尔运算操作有优先运算顺序，优先级由高到低依次为 not、and 或 near、or。采用运算优先规则后，运算符按照从左至右的顺序被处理。对于要先于其他查询的执行部分，可以使用括号()来超越普通优先级。例如，下面前三个查询是等价的，而第四个不是：

- a and b or c
- c or a and b
- c or（a and b）
- （c or a）and b

在第四个查询中，首先计算 or 运算符的值，因为表达式在括号中。

注意：如果查询短语中包含布尔运算符，应在该短语两端加引号。例如，“horse and rider”被认为是一个短语，而不是布尔逻辑表达式。

4. 关系运算符

使用关系运算符查询，可以查找属性值与指定关系相匹配的文档，如表 10-7 所示。例如，使用@DocPageCount>6 可查询所用超过 6 页的文档。

表 10-7　关系运算符说明

运算符	说　明	运算符	说　明
<	小于	>=	大于或等于
<=	小于或等于	>	大于
=	等于	!=	不等于

当与向量一起使用时，关系运算符用于相应的向量元素测试。如果所有单独测试都通过，向量之间的关系就成立。

例如，两个向量 A｛a1，a2，a3｝和 B｛b1，b2，b3｝，A>B 成立的充分必要条件是 a1>b1、a2>b2、a3>b3 同时成立。

如果一个向量的元素比其他向量的元素多，则只测试匹配的元素，其他元素将被忽略。

5. AllOf 和 SomeOf 运算符

当执行矢量属性比较时，AllOf（^a）和 SomeOf（^s）运算符可以和关系运算符一起使用。当使用 AllOf 运算符时，关系运算符左边的每个向量元素必须通过与右边的每个向量



元素的比较；当使用 SomeOf 运算符时，至少应有一个向量元素必须符合比较测试才能通过如表 10-8 所示。

表 10-8　AllOf 和 SomeOf 运算符范例

测　试	结　果
(1,2,3)^a>(1,2)	因为左边的第一个元素不比右边的第一个元素大，所以测试失败
(1,2,3)^s>(2,1)	因为左边的第三个元素比右边的第一个元素大，所以测试通过

除了传统的关系运算符之外，AllOf 和 SomeOf 运算符允许按位比较属性值，从而可以使用位比较符进行查询，如表 10-9 所示。

表 10-9　位比较符范例

格　式	结　果
@attrib^a 0x820	索引服务只查找存档为属性的打开的压缩文档
@attrib^s 0x20	索引服务查找存档为属性的打开的压缩文档和文档

6. Contains 和 Equals 运算符

使用 Contains 运算符可搜索特定属性内的任意词或词组。如果没有指定运算符，将假定为 Contains 运算符。

例如，查询 @DocTitle “the red dog”或 @DocTitle Contains “the red dog”，标题属性值为 The story of the red dog 的文档将满足上面的查询。

Equals 运算符用来指定属性值必须准确匹配查询中的字或词。短格式是等号“＝”。例如，@DocTitle ＝ “the red dog”或 @DocTitle Equals “the red dog”，只有标题属性值是 the red dog 的文档才满足这一查询。标题为 The story of the red dog 的文档将不符合该查询，因为它含有查询中没有的单词。

注意：要搜索字“contains”或“equals”，必须使用引号。

7. 通配符和变形词格式的查询

在查询中可以使用星号“＊”和问号“?”作为通配符来查询所需内容。星号代表任意字符序列，问号代表任一字符。例如，查询 esc＊，将匹配 escarpment、escape 等词条。查询 r?n，将匹配 run 和 ran，但不匹配 ruin。

对于变形词格式查询，索引服务将搜索所给出单词的其他形式。变形格式可以是查询词的变形版本或使用查询词作为前缀的词。例如查询 swim＊＊，变形格式将产生变形匹配：swimming、swam 和 swum。

下面介绍微软索引服务提供的几种查询类型。

(1) 自由文本查询

自由文本查询是最常用的查询方式，如表 10-10 所示。在自由文本查询中，可以输入一组单词或一个完整的句子。索引服务将查找与自由文本查询中的单词或短语最匹配的页。自由文本查询以 $contents 为前缀。



表 10-10　自由文本查询范例

查询内容	范　　例	结　　果
匹配自由文本的文档	$contents How do I print in Microsoft Excel? 或 How do I print in Microsoft Excel?	提到 printing 和 Microsoft Excel 的页

提示：如果在没有指定查询类型或属性的情况下只提交查询文本，索引服务在默认情况下会使用自由文本查询和 Contents 属性。

注意：在自由文本查询中，逻辑、相近和通配运算符都将被忽略。

（2）词组查询

搜索特定的词语或短语，可以使用词组查询。词组查询以@contents 为前缀，或者也可用引号（“”）将特定词组引起来进行查询。词组查询中的单词必须以输入的顺序出现在文档中，没有插入的单词，如表 10-11 所示。

表 10-11　词组查询范例

查询内容	范　　例	结　　果
匹配特定词组的文档	@contents big red truck 或 “big red truck”	含有词组 big red truck 的页

提示：当使用词组查询时，单词的序列和位置对确定文档是否匹配查询很重要。词组查询还可用来搜索文档的内容与属性值。

注意：在词组查询中，例外列表中的单词按占位符处理。例如，如果查找 Word for Windows，其结果应该是 Word for Windows 和 Word and Windows，因为 for 出现在例外列表中。

（3）匹配查询

最简单的模式匹配查询类型是使用带通配符字符（如星号“*”和问号“?”）或变形词格式的单词或单词片段的查询。稍复杂匹配查询类型是使用带表达式的查询。在表达式中，可以指定各类属性和使用各种运算符，以便匹配文档的各项属性，精确查找含有与所给条件相匹配的属性值的文件。

表达式可分为两种类型：关系表达式和常规表达式。

① 关系表达式以 at 符号“@”开头，后跟属性名、关系运算符和属性值，通常用在特定值的比较中，如表 10-12 所示。例如，要查找大小超过 1MB 的文件，可以执行查询@size>1 000 000。

表 10-12　关系表达式示例

查 询 内 容	范　　例	结　　果
匹配某词语的文档	@contents white cat	包含词组 white cat 的页
大于指定值	@size > 1 000 000	大小超过 1MB 的文档
等于指定值	@DocAuthor = Michael Smith	由 Michael Smith 创作的文档



续表

查询内容	范　例	结　果
在特定日期和时间后修改的文档	@write > 96/2/14 13:00:00	在 1996 年 2 月 14 日 13 点后修改的文档
在相对日期之后修改过的文档	@write > -1d2h	在最近 26 小时之内修改过的文档
匹配一个矢量的矢量	@vectorprop = { 10, 15, 20 }	向量值为{ 10, 15, 20 }的 ActiveX 文档
每一个值都符合条件的矢量	@vectorprop >^a 15	向量中所有值都大于 15 的 ActiveX 文档
至少有一个值符合条件的矢量	@vectorprop =^s 15	向量中的值至少有一个值大于 15 的 ActiveX 文档
匹配布尔与关系运算的文档	Microsoft and @size > 1 000 000	包含单词"Microsoft",并且大小大于 1MB 的页

技巧:

- 在表示相对于当前的日期和时间时,可以通过在负号"-"后紧跟一个或多个整数和时间单位来表示。时间单位的表示为:y 代表年,q 代表季度(三个月),m 代表月,w 代表周,d 代表天,h 代表小时,n 代表分,s 代表秒。例如,@write > -1d2h。
- 货币值为 x.y 格式。在此,x 是全额的整数值,y 是小数值。单位没有假定值。
- 逻辑值为 TRUE 和 FALSE。
- 向量(VT_VECTOR)表示为:左大括号"{"开始、紧跟逗号分隔的值列表,右大括号"}"结束。

② 常规表达式以号码符号"#"开头,后面有属性名和属性值,如表 10-13 所示。例如,要查找所有视频(.avi)文件,可以执行查询 #filename *.avi。

常规表达式是一些符号集,用于匹配各种内容的查询。常规表达式包括星号"*"、问号"?"和竖线"|",除此以外的任何字符均默认与自身匹配。如果属性查询中包含星号"*"、问号"?"或竖线"|",则无论表示哪种模式,该查询都将被自动作为常规表达式处理。

注意:在常规表达式中不能使用 Contents 和 All 属性。

表 10-13　常规表达式示例

查询内容	范　例	结　果
以特定前缀开始的值	#DocAuthor George*	作者名字是以 George 开头的文档
带有扩展名集中任何一种扩展名的文件	#filename *.|(exe|,dll|,sys|)	扩展名为 .exe、.dll 或 .sys 的文件
一组带有指定文件名的文件	#filename = *|(ss|,ing|).cxx	返回所有文件名以 ss 或 ing 结尾、扩展名为 cxx 的文档
not 运算符(^)	#filename = |[^f]*.cxx	返回所有文件名以非 f 的任何字母开头、扩展名为 cxx 的文档
范围匹配	#filename = |[a-d]*.cxx	返回所有文件名以 a 到 c 的某个字母开头、扩展名为 cxx 的文档

续表

查询内容	范　例	结　果
精确计数匹配	#filename = *s|{2|}.cxx	返回所有文件名正好以两个 s 结尾、扩展名为 cxx 的文档
零个或多个匹配	#filename = c|*ss.cxx	返回所有文件名以零个或多个 c 字符开头、以 ss 结尾、并且扩展名为 cxx 的文档。文件 ss.cxx、css.cxx 和 cccccss.cxx 符合条件，但 cctss.cxx 不符合条件
零个或一个匹配	#filename = c|? ss.cxx	返回所有文件名以零个或一个 c 字符开头、以 ss 结尾、并且扩展名为 cxx 的文档。文件 ss.cxx 和 css.cxx 符合条件
一个或多个匹配	#filename = c|+ss.cxx	返回所有文件名以一个或多个 c 字符开头、以 ss 结尾、并且扩展名为 cxx 的文档。文件 css.cxx 和 cccccss.cxx 符合条件，但 cctss.cxx 和 ss.cxx 不符合条件
指定扩展名的文件	#filename *.avi	扩展名为.avi 的文件
匹配关系与常规运算的文档	@size<100 and #filename *.gif	小于 100 字节的 GIF 文件

技巧：

- 字符“*”、“.”和“?”的作用与它们在 Windows 中的作用一样，星号匹配任意字符，句号匹配(.)或字符串结尾，问号匹配任何单个字符。
- 常规表达式可以放在匹配的引号中（“”）。要在查询中使用特殊的字符，如“&”、“|”、“^”、“#”、“@”、“$”、“(”、“)”等，也应用引号(“”)将查询括起来。
- 字符“|”是转意字符，在“|”之后的字符具有特殊含义：

  “(”开始一个组，后面必须有“)”相对。

  “)”结束一个组，前面必须有“(”相对。

  “[”开始一个字符类，后面必须有“]”(不转意)相对。

  “{”开始计数的匹配，后面必须有“}”相对。

  “}”结束计数的匹配，前面必须有“{”相对。

  “,”分隔 or 子句。

  “*”匹配前面表达式的零次或多次出现。

  “?”匹配前面表达式的零次或一次出现。

  “+”匹配前面表达式的一次或多次出现。

  其他字符，包括“|”，匹配自己。
- 方括号（[]）之间的下列字符具有特殊含义：

  “^”除了下面的类，匹配任意。它必须是第一个字符。

  “]”匹配]。只能在“^”之后，否则起结束类的作用。

  “—”范围运算符。前面和后面可以是普通字符。

  其他的匹配自己(范围的开始或结束)。



- 大括号（{}）之间适用下列语法：
  |{m|}精确匹配前面表达式的 m 次出现(0<m<256)。
  |{m,|}匹配前面表达式的至少 m 次出现(1<m<256)。
  |{m,n|}匹配前面表达式从 m 到 n 次的出现，包含 m 和 n(0<m<256,0<n<256)。
- 要匹配“*”、“.”和“?”，应用方括号([])括起来(例如，[?]hello 将匹配“? hello”)。

（4）向量空间查询

向量空间查询将返回匹配词和词组列表的文档。由向量空间查询返回的文档不必与查询中的每一项目都匹配。每个文档的等级表明文档与查询的匹配情况，如表 10-14 所示。

表 10-14　向量空间查询范例

搜索目标	示　　例	结　　果
包含指定单词的文档	light，bulb	包含要搜索的这两个词中任意一个或两个都包含的文档。包含这两个词的文档比那些仅包含一个词的文档等级要高
包含前缀、加权的词和短语的文档	invent *，{weight value=.3} light，{weight value=.1} bulb，{weight value=.6}“light bulb”	包含有前缀 invent 的单词、单词 light、bulb 和短语 light bulb 的文档。包含词 light 的文档级别比包含词 bulb 的高，但低于包含短语 light bulb 的文档级别

可以使用{weight}标记加权查询词条来设置相对重要性，以影响结果的排列。该标记出现在查询词条之前，无结束标记。用法为{weight value = n} 查询词条。

其中，value 参数指定分配给查询条件的相对权值。该值可以在范围 0.0 到 1.0 之间变动。如果没有指定权值，索引服务默认使用权值 1.0。

例如，下面是一个带权值的查询：

```
{weight value = .250}dog and {weight value = .500}cat and {weight value = 1.000}pig
```

该查询中包含词 pig 的文档级别应比包含词 cat 的文档级别高，以此类推，包含词 cat 的文档级别应该比包含词 dog 的文档级别高。

技巧：向量空间查询中的组件以逗号隔开，组件可以用 [weight]语法加权。当结果按等级排序时，向量空间查询最好。

10.6　疑难解答

（1）如何自定义设置被索引的目录？

打开【索引服务】节点，在系统编录或新创编录中，可根据实际情况增减被索引的目录范围。

（2）如何控制索引服务对系统资源的影响？

索引服务器提供了相应设置，即【调整性能】命令来控制其对系统资源的使用。在【索引





服务用法】对话框中,可通过对“索引”和“查询”选项进行不同的设置,来改变索引服务对系统资源的占用。另外,也可提高和降低索引和查询过程的优先级。

(3) 在 NTFS 文件系统中,如何控制指定文档不被索引?

通常有三种方式:

① 在编录节点的目录列表中打开【添加目录】对话框进行设置。

② 设置文件夹或文档的高级属性,来改变其是否能被索引。

③ 设定访问特权,若用户没有对某文档的读权限,将无法在索引结果中看到该文档。也可不提供某特定文档的过滤器使其不被索引。

(4) 如何在索引查询中使用模糊查询?

在微软索引服务提供的查询方式中,可以使用传统匹配符(“ * ”和“?”)来进行模糊查询,还可以生成某个单词的语法变化形式来扩大查询的范围,即变形方式来进行查询(例如查询 swim ** ,变形格式将产生变形匹配 swimming、swam 和 swum)。

习　　题

1. 填空题

(1) 搜索引擎按其工作方式主要可分为三种类型,分别是________、________和________。

(2) 在索引服务的工作机制中,索引过程的实现包括________、________和________三个主要步骤。

2. 选择题

(1) 互联网上第一个中文搜索引擎是(　　)。

A. Yahoo　　B. Sohu　　C. 新浪　　D. 天网

(2) 除括号“()”能超越普通优先级外,下列(　　)运算符优先级最高。

A. not　　B. and　　C. near　　D. or

3. 思考题

(1) 如何在索引服务中控制某文件夹不被索引?

(2) 微软索引服务支持哪些查询方式?

4. 上机题

(1) 创建一个编录名为 test 的索引,将索引文件放于自建的 index 文件夹下,然后将 C 盘添加到该编录的作用域内,并将 Windows 文件夹排除在该编录的索引范围之外。

(2) 查询所有文件名包含 inf,大小超过 100kb,且扩展名为.dll 的文件。

参 考 文 献

[1] 陈洪彬.前沿流媒体实用手册.北京：中国科学技术出版社,2003
[2] 康瑞锋.全国网络技术水平考试二级学员教材.北京：电子工业出版社,2006
[3] 王春海.非常网管——网络应用.北京：人民邮电出版社,2007
[4] 康瑞锋.计算机网络操作系统实用教程.南京：东南大学出版社,2007
[5] 唐涛等.新世纪 Windows Server 2003 应用教程.北京：电子工业出版社,2006
[6] 王鲜芳.Windows Server 2003 组网教程.北京：电子工业出版社,2005
[7] 贾振刚.Windows Server 2003 网络基础实用教程.武汉：华中科技大学出版社,2009
[8] 贾振刚.Windows Server 2003 管理与应用项目教程.北京：中国电力出版社,2009
[9] 鞠光明,刘勇.Windows 服务器维护与管理教程与实训.北京：北京大学出版社,2005
[10] 王文寿.网管员必备宝典——Windows Server 2003 网络管理.北京：清华大学出版社,2007
[11] 王隆杰.Windows Server 2003 网络管理实训教程.北京：清华大学出版社,2006
[12] 戴有炜.Windows Server 2003 用户管理指南.北京：清华大学出版社,2004
[13] 钟小平,张金石.网络服务器配置与应用.3 版.北京：人民邮电出版社,2007
[14] 高晓飞.网络服务器配置与管理:Windows Server 2003 平台.北京：高等教育出版社，2009
[15] 崔奎勇.网络服务器配置——Windows Server 2003 .北京：清华大学出版社,2009
[16] http://stu.gzeic.com/
[17] http://windows.jnrp.cn/
[18] http://www.sxszjzx.com/
[19] http://www.webth2.cn/